Army Regulation 25–2

Information Management: Management of Subdisciplines

Information Assurance

Headquarters
Department of the Army
Washington, DC
14 November 2003

UNCLASSIFIED

SUMMARY of CHANGE

AR 25–2
Information Assurance

This regulation--

o Supersedes AR 380-19, HQDA LTR 25-02-1, and HQDA LTR 25-03-1.

o Introduces and implements the concept of Defense in Depth (paras 1-1g and 1-4e).

o Introduces the concept of Information Assurance Best Business Practices to facilitate the Army's ability to adapt to changing technology or implementation guidance (para 1-1g(13)).

o Changes the titles of personnel charged with implementing and enforcing the policy from Information Systems Security to Information Assurance (chap 2).

o Adds and defines the Information Assurance personnel hierarchy (chap 2).

o Changes the terminology for information technology professionals from "automated data processing" to "information technology" (chap 2).

o Adds requirements for Communications Security Logistics Activity for an Army cryptographic applications certification process and involvement in life-cycle management of information systems (para 2-14).

o Introduces the concepts of mission assurance category, levels of confidentiality, and levels of robustness of information and systems (para 4-4).

o Outlines monitoring guidelines and requirements (para 4-5t).

o Adds a linkage to tie in the intelligence threat support requirements in AR 381-11 to the duties of the program executive officer and the program manager to enable consideration of foreign-origin information operations threats early in the development or acquisition of Army automated information systems (para 4-6d).

o Imposes more robust password requirements (para 4-12).

o Outlines personnel security requirements for information technology positions (paras 4-14c(5) and (6)).

o Introduces Army Web Risk Assessment Cell (para 4-20g(16)).

o Changes Information Assurance Vulnerability Assessment Program to Information Assurance Vulnerability Management Program (paras 4-24 through 4-26).

o Supplements the DOD Information Technology Security Certification and Accreditation Process to add a threat analyst to the team that develops the System Security Authorization Agreement for the Army (para 5-1c).

Headquarters
Department of the Army
Washington, DC
14 November 2003

***Army Regulation 25–2**

Effective 14 November 2003

Information Management: Management of Subdisciplines

Information Assurance

By order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

Joel B Hud

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army

History. This is a new Department of the Army regulation.

Summary. This regulation provides Information Assurance policy and mandates procedures for implementing the Army Information Assurance Program, consistent with today's technological advancements, in a generic fashion to avoid dependency on specific technology. It establishes policies and assigns responsibilities for achieving acceptable levels of Information Assurance in engineering, implementation, operation, and maintenance for all information systems connecting to or crossing any U.S. Army-managed network. It provides administrative and systems security requirements, including those for interconnected systems. It defines and mandates the use of risk assessments and the Defense in Depth Strategy. It describes the roles and responsibilities of the individuals who constitute the Information Assurance security community and its users, and outlines training and certification requirements. It requires a life-cycle management approach to implementing Information Assurance requirements and requires the implementation of a configuration management process. It establishes a procedure to document the status of generic accreditations for all information systems fielded by Department of the Army organizations, DA-chartered program managers, and Headquarters, Department of the Army staff proponents. It also establishes requirements to ensure that Department of Defense and Army-level designated approving authorities meet the system accreditation policies of this regulation before fielding or testing any system that requires connection to a military network.

Applicability. This regulation applies to all users, information, information systems, and networks, at all classification levels, of the Active Army, Army National Guard, U.S. Army Reserve, program executive officers, direct reporting program managers; strategic, tactical, and non-tactical environments; camps, posts, and stations; internal or external organizations, services, tenants, or agencies (for example, DOD, sister Services, U.S. Army Corps of Engineers (USACE); Army and Air Force Exchange Service (AAFES); morale, welfare, and recreation activities; educational institutions or departments (for example, DOD schools, the U.S. Military Academy at West Point); and Army affiliated or sponsored agencies (for example, Western Hemisphere Institute for Security Cooperation). This regulation remains in effect, without change, during mobilization, deployment, or national emergency.

Proponent and exception authority. The proponent for this regulation is the Chief Information Officer/G–6 (CIO/G–6). The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The proponent may delegate this approval authority, in writing, to an individual within the proponent agency in the grade of colonel or above or the civilian grade equivalent.

Army management control process. This regulation contains management control provisions and identifies key management controls that must be evaluated. A management control evaluation checklist appears at appendix C.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Chief Information Officer, G–6, 107 Army Pentagon, Washington DC 20310–0107.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to CIO/G–6, 107 Army Pentagon, Washington DC 20310–0107.

Distribution. This publication is available in electronic media only and is intended for command levels B, C, D, and E for the Active Army, the Army National Guard of the United States, and the U.S. Army Reserve.

*This publication supersedes AR 380–19, 27 February 1998; HQDA LTR 25–02–1, 15 April 2002; HQDA LTR 25–03–1, 23 April 2003.

Contents (Listed by paragraph and page number)

Contents—Continued

Contents—Continued

Chapter 6
Communications Security, *page 42*

Chapter 7
Risk Management, *page 45*

Appendixes

Table List

Figure List

Glossary

Chapter 1
Introduction

1–1. Purpose

This regulation establishes Information Assurance (IA) policy, roles, and responsibilities.

a. It establishes policies and assigns responsibilities for all users and developers for achieving acceptable levels of IA in the engineering, implementation, operation, and maintenance (EIO&M) for all information systems (ISs) across the U.S. Army Enterprise Infostructure (AEI). Such ISs include, but are not limited to, computers, processors, devices, or environments (operating in a prototype, test bed, stand-alone, integrated, embedded, or networked configuration) that store, process, access, or transmit data, including unclassified, sensitive (formerly known as sensitive but unclassified (SBU)), and classified data, with or without handling codes and caveats. ISs used for teleworking, telecommuting, or similar initiatives; contractor owned or operated ISs; ISs obtained with non-appropriated funds; automated tactical systems (ATSs); automated weapons systems (AWSs); distributed computing environments (DCEs); and systems processing intelligence information are required to adhere to the provisions of this regulation.

b. Commanders of activities requiring limited access by local foreign national officials or personnel (including IT positions) will follow the provisions of this regulation.

c. This regulation applies equally to the operation, safeguarding, and integrity of the infrastructures (for example, power, water, air conditioning), including the environment in which the IS operates.

d. While no regulation or policy on security measures can ever provide a 100% solution, implementation of the concepts, procedures, and recommendations in this regulation will drastically reduce the manageability requirements of assets, and minimize the effects of unauthorized access or loss. The cornerstone philosophy of Army IA is to design, implement, and secure access, data, ISs, and data repositories; increase trust and trusted relationships; employ technical and operational security mechanisms; deny all unauthorized accesses; and permit necessary exceptions to support Army, DOD, and Joint interagency and multinational (JIM) tactical and sustaining-base operations.

e. Army information constitutes an asset vital to the effective performance of our national security roles. While all communication systems are vulnerable to some degree, the ready availability as low-cost, information technology and attack tools, increased system connectivity and asset distribution, and standoff capabilities make computer network attacks (CNAs) an attractive option to our adversaries. Information Assurance capabilities and actions protect and defend network availability, protect data integrity, and provide the ability to implement effective computer network defense (CND). Management of Army information is imperative so that its confidentiality, integrity, availability, and non-repudiation can be ensured, and that users of that data can be properly identified and authenticated.

f. The AEI architecture requires the establishment, verification, and maintenance of trusted enclaves, trusted connectivity, and trusted information and information sources along with the capability to access and distribute that information by leveraging technology and capabilities to amplify that trust.

g. To accomplish these foundational objectives, this regulation establishes requirements as follows—

(1) Provides administrative and systems security requirements, including those for interconnected systems.

(2) Defines and mandates the use of risk assessments.

(3) Defines and mandates the Defense in Depth strategy.

(4) Promotes the use of efficient procedures and cost-effective, computer-based security features and assurances.

(5) Describes the roles and responsibilities of the individuals who constitute the IA security community and its system users, and outlines training and certification requirements.

(6) Requires a life-cycle management approach to implementing IA requirements.

(7) Introduces the concepts of mission assurance category, levels of confidentiality, and levels of robustness of information.

(8) Implements DOD Directive 8500.1, DOD Instructions (DODIs) 8500.2 and DODI 5200.40, and Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01 to align Army IA goals and requirements to support the DOD Information Management Strategic Plan.

(9) Establishes a procedure to document the status of accreditations for all ISs fielded by DOD organizations, Army chartered program managers (PMs), and HQDA staff proponents.

(10) Ensures DOD and Army-level designated approving authorities (DAAs) meet the system accreditation polices of this regulation before fielding or testing any system that requires connection to an Army network.

(11) Requires the implementation of a Configuration Management Process.

(12) Describes the Continuity of Operations Plan (COOP).

(13) Establishes and implements the concept of Best Business Practices (BBPs) to define and enforce mandatory and specific measures, practices, or procedures to meet changing technology or IA requirements.

(14) Provides the foundation for the Networthiness Certification Program.

h. Other policies, procedures, or directives also govern certain systems. In the event of conflicts among these policies, procedures, or directives, the more stringent requirement will take precedence. When the most stringent policy cannot be determined, major Army commands (MACOMs), directors of information management (DOIMs), regional chief information officers (RCIOs), functional proponents, or others will submit a request for a policy decision through their RCIO to the Chief Information Officer/G–6 (CIO/G–6).

i. The mention of commercial products in this regulation does not imply endorsement by either DOD or the U.S. Army.

j. This regulation is punitive in nature. Violations of paragraphs 3–2, 3–3, 4–5, 4–6, 4–7, 4–10, 4–11, 4–12, 4–13, 4–16, 4–17, 4–18, 4–20, 4–21, 4–22, 4–23, 4–25, 4–30, 6–1, 6–2, and 6–5 of this regulation may be punished as violations of a lawful general order under Article 92 of the Uniform Code of Military Justice (UCMJ) or under other disciplinary, administrative, or contractual actions as applicable. These cited paragraphs and other provisions of this regulation might be the basis for a commissioned, warrant, or noncommissioned officer to issue a lawful order to a soldier. Penalties for violations of the above-cited provisions of this regulation, and orders based on these and other provisions of this regulation, include the full range of statutory and regulatory sanctions. Personnel not subject to UCMJ who fail to comply with these requirements are subject to disciplinary, administrative, or prosecutorial actions as authorized from criminal or civil sanctions under sections including, but not limited to, the United States Code, contractual support obligations, or Federal or state regulations.

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms

Special terms and abbreviations are identified in the glossary.

1–4. Army Information Assurance Program

a. The Army Information Assurance Program (AIAP) is a unified approach to protect unclassified, sensitive, or classified information stored, processed, accessed, or transmitted by Army ISs, and is established to consolidate and focus Army efforts in securing that information, including its associated systems and resources, to increase the level of trust of this information and the originating source. The AIAP will secure Army ISs through IA requirements, and does not extend access privileges to special access programs (SAPs), classified, or compartmentalized data; neither does it circumvent need-to-know requirements of the data or information transmitted.

b. The AIAP is designed to achieve the most effective and economical policy possible for all ISs using the risk management approach for implementing security safeguards. To attain an acceptable level of risk, a combination of staff and field actions is necessary to develop local policy and guidance, identify problems and requirements, and adequately plan for required resources.

c. Information systems exhibit inherent security vulnerabilities. Cost-effective, timely, and proactive IA measures and corrective actions will be established and implemented to mitigate risks before exploitation and to protect against vulnerabilities and threats once they have been identified.

(1) Measures taken to attain IA objectives will be commensurate with the importance of the operations to mission accomplishment, the sensitivity or criticality of the information being processed, and the relative risks (threats and vulnerabilities) to the system. Implementation of an IA operational baseline should be an incremental process of protecting critical assets or data first, and then building upon those levels of protection and trust across the enclave.

(2) Statements of security requirements will be included in the earliest phases (for example, mission needs statements, operational requirements document, capstone requirement document) of the system acquisition, contracting, and development life cycles.

d. An operationally focused IA program requires the use of innovative approaches (herein referred to as BBPs) in establishing and implementing the best ideas, concepts, and methodologies from both industry and U.S. Army resources. Best Business Practices (BBPs) allow transitional growth in Army IA initiatives to integrate, use, and modify technological or procedural changes into mandatory improvements.

e. The elements of the DiD strategy focus on three areas: people, operations, and defense of the environment (the latter of which encompasses the computing environment, the networks, the enclave boundaries, and the supporting infrastructure).

f. The AIAP is not a stand-alone program, but incorporates related functions from other standards or policies such as operations security (OPSEC), communications security (COMSEC), transmission security (TRANSEC), information security (INFOSEC), and physical security to achieve IA requirements.

g. Failure to implement proactive or corrective IA security measures, guidance, policy, or procedures may prevent system or enclave accreditation, installation, or operation. IA or network personnel may block access to ISs that reflect poor IA security practices or fail to implement corrective measures. Users in violation of policies or procedures may receive disciplinary actions under the UCMJ, federal, or state criminal statutes and laws.

Chapter 2
Responsibilities

2–1. The Chief Information Officer/G–6

In addition to the responsibilities defined in paragraph 2–2, the Chief Information Officer/G–6 (CIO/G–6) as the functional proponent for Information Assurance will—

a. Establish and issue Army IA policy and procedures and serve as the focal point for Army IA programs and funding.

b. Develop, review, and coordinate Army input into DOD IA policy documents.

c. Establish and maintain Army standardized evaluations and test methodology certification procedures and security requirements as part of the accreditation process.

d. Document, develop, coordinate, present, prioritize, and defend Army IA resource requirements in the planning, programming, and budgeting process.

e. Coordinate with the DCS, G–2 for the policy, development, dissemination, support, tactics, techniques, and procedures for the design, implementation, and operation of the key management infrastructure (KMI) and systems to support Army encryption requirements.

f. Provide program oversight for Army implementation of the KMI and funding aspects of the Electronic Key Management System (EKMS).

g. Prepare the annual Army IA readiness report.

h. Provide technical and operational assistance and support to the United States Army Audit Agency (USAAA) in its audits and reviews of Army ISs.

i. Evaluate technological trends in IA and establish a methodology to integrate advancements.

j. Provide IA guidance to Army elements in identifying and incorporating requirements consistent with the KMI requirements in project development.

k. Act as the DAA for classified systems developed by the DA staff agencies as well as systems developed by PEOs or PMs that are generically accredited to operate at Protection Level (PL) 4 in accordance with Director of Central Intelligence Directive (DCID) 6/3.

l. Provide a point of contact (POC) with the Defense Information Systems Agency/Center for Information Systems Security (DISA/CISS) for advice and assistance and implementation of certification tests and programs for Army operated ISs.

m. Serve as the Army member of the Committee on National Security Systems (CNSS) and the Subcommittees for Telecommunications Security (STS) and Information Systems Security (SISS).

n. Provide an Army voting member to the Key Management Executive Committee (KMEC) and Joint Key Management Infrastructure Working Group (JKMIWG).

o. Provide policy, guidance, and oversight on the employment of National Institute of Standards and Technology (NIST) approved cryptography for the protection of unclassified and sensitive information.

p. Appoint the Chairperson and Alternate Chairperson for the Tier 1 System Management Board (TSMB), which has operations management responsibilities for the Tri-Service EKMS Common Tier 1 System (CT1S).

q. Participate with the Deputy Chief of Staff, G–2 (DCS, G–2); U.S. Army Intelligence and Security Command (USAINSCOM); Network Enterprise Technology Command/9th Army Signal Command (ASC) (NETCOM/9th ASC); 1st Information Operations (LAND) Command (1st IO CMD (LAND)); and the U.S. Army Criminal Investigation Command (CID) in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which IA countermeasures should be directed.

r. Maintain a list of DAAs for all systems fielded by a DA staff element or by a DA-chartered PM.

s. Ensure the concepts of, and strategies within, this regulation are utilized as the basis for networthiness certification.

t. Provide technical and operational assistance and support to the Army Web Risk Assessment Cell (AWRAC).

u. Provide program oversight of Communications Security Logistics Activity (CSLA) for an Army cryptographic applications certification process (when developed).

2–2. Principal HQDA officials and staff

Principal HQDA officials and staff, within their respective areas of functional or process proponency, will implement IA requirements within their respective functional areas. As HQDA proponents, these individuals will—

a. As required in their functional area, develop, coordinate, supervise, execute, and allocate the research, development, test, and evaluation (RDT&E) procurement resources in support of IA program requirements.

b. Participate collectively with other Army IA stakeholders in the enterprise planning, acquisition, and operation of IA strategies.

c. Integrate approved IA tools, doctrine, procedures, and techniques into all ISs under their purview.

d. Establish procedures for reporting security incidents and violations in accordance with Section VIII, Incident and Intrusion Reporting.

e. Support the Army's Information Assurance Vulnerability Management (IAVM) Program notification and correction processes. IAVM notification and correction are DOD and Army operational requirements.

f. Develop and implement local Acceptable Use Policy (AUP) for all users authorized access to Army ISs (appendix B presents a sample AUP).

g. Ensure all systems, for which the principal HQDA Army office is the proponent or sponsor, are accredited and re-accredited in accordance with DODI 5200.40 (DITSCAP) and that Army specific requirements are approved through NETCOM, CIO/G–6, and MACOM Information Assurance Program Managers (IAPMs) not less than 3 months before proposed fielding, operating, or upgrading.

h. Appoint appropriate IA personnel per chapter 3 of this regulation and provide CIO/G–6 a copy of the appointment orders.

i. Identify personnel and procedures at all organizational and subordinate levels, as required, to implement a Configuration Management Board (CMB) or Configuration Control Board (CCB) to effect control and management mechanisms on all ISs, devices, configurations, and IA implementations. Include IA personnel as members of the board.

j. Incorporate related OPSEC, COMSEC, and INFOSEC policies and requirements into a comprehensive IA management program.

2–3. The Assistant Secretary of the Army for Acquisition, Logistics, and Technology

In addition to the responsibilities defined in paragraph 2–2, the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA (ALT)) will—

a. Forward to National Security Agency (NSA) and HQDA approved materiel requirements for IA tools and equipment (including cryptographic equipment), along with requests for RDT&E efforts to fulfill those needs.

b. Designate an Army materiel developer to conduct and update threat analyses as outlined by AR 381–11.

c. Monitor NSA, other Service COMSEC, and IA RDT&E projects that are of interest to the Army. Designate an Army integrating agency as defined in AR 70–1 for each project having potential application for Army use. Require the designated agency to maintain liaison with the developing agency and inform interested Army agencies of the progress of such projects.

d. Establish coordination with NSA concurrent life-cycle management milestones for development of cryptographic equipment in support of IA initiatives.

e. Conduct research and acquire basic knowledge of the techniques and the circuitry required to provide an effective CND capability in appropriate types of Army equipment.

f. Ensure application of capabilities to perform IS risk analysis, reduction, and management.

g. Ensure that Army PEOs and PMs include IA in all systems development activities.

2–4. The Deputy Chief of Staff, G–2

In addition to the responsibilities defined in paragraph 2–2, the Deputy Chief of Staff, G–2 (DCS, G–2) will—

a. Coordinate the development and dissemination of DOD, national, theater, and DA-level IA threat information to the Army.

b. Coordinate with the CIO/G–6 for the policy, development, dissemination, support, tactics, techniques, and procedures for the design, implementation, and operation of the Key Management Infrastructure (KMI) and systems to support Army encryption requirements.

c. Develop policy for safeguarding and controlling COMSEC and controlled cryptographic item (CCI) material.

d. Ensure all intelligence systems, for which the DCS, G–2 is the Army proponent or sponsor, are accredited or re-accredited in accordance with DCID 6/3.

e. Ensure that the Department of Defense Intelligence Information System (DODIIS) Program is implemented and guidance is published.

f. Serve as the approval authority for external IS penetration and exploitation testing of operational networks.

g. Participate with the CIO/G–6, USAINSCOM, NETCOM/9th ASC, 1st IO CMD (LAND), and CID in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which IA countermeasures should be directed.

2–5. The Deputy Chief of Staff, G–3

In addition to the responsibilities defined in paragraph 2–2, the Deputy Chief of Staff, G–3 (DCS, G–3) will—

a. Support the CIO/G–6 in the accomplishment of Army IA responsibilities.

b. Ensure IA training is integrated throughout the Army.

c. Support audits and reviews of Army ISs and networks through operational and technical assistance, as required.

d. Provide guidance, requirements, and oversight for Information Operations Condition (INFOCON) alerting and implementation measures.

e. Provide guidance, requirements, and oversight for OPSEC measures to support an IA management policy.

2–6. The Deputy Chief of Staff, G–4

In addition to the responsibilities defined in paragraph 2–2, the Deputy Chief of Staff, G–4 (DCS, G–4) will—

a. As the Army independent logistician, develop logistics policies (including integrated logistics support policy), concepts, procedures, and guidance for logistics support of IA equipment used in support of all Army missions.

b. Prescribe execution of NSA or DOD logistics management directives that apply to classified COMSEC and CCI materiel.

c. Prescribe and supervise the implementation of procedures for property control and the accounting of CCI materiel during distribution, storage, maintenance, use, and disposal. All guidance will conform to the security standards developed by the DCS, G–2 for safeguarding COMSEC and CCI materiel.

d. Supervise logistics support planning to ensure the availability of materials and publications needed for repair, test measurement, and diagnosis of IA equipment and systems.

e. Provide continuous logistical support for fielded IA material and test equipment.

2–7. Commanders of MACOMs; Chief, Army Reserve (CAR); Chief, National Guard Bureau (NGB); program executive officers (PEOs); direct reporting program managers; NETCOM RCIOs; direct reporting units (DRUs); Installation Management Agency (IMA); and the Administrative Assistant to the Secretary of the Army

Commanders of MACOMs; Chief, Army Reserve; Chief, National Guard Bureau; Program Executive Officers; direct reporting program managers (PMs not under the PEO structure); NETCOM RCIOs; direct reporting units; Installation Management Agency; and the Administrative Assistant to the Secretary of the Army (acting as the senior official for all HQDA administrative and management services), in addition to the responsibilities defined in paragraph 2–2, will—

a. Develop and implement an IA program with the hardware, software, tools, personnel, and infrastructure necessary to fill the IA positions and execute the duties and responsibilities outlined in this regulation.

b. Oversee the maintenance, documentation, and updating of the certification and accreditation (C&A) requirements required for the operation of all ISs as directed in this regulation.

c. Implement and manage IT system configurations, including performing IAVM processes as directed by this regulation.

d. Appoint IA and other personnel (for example, alternates) to perform the duties in chapter 3 of this regulation and provide IAPM POC information to the NETCOM RCIO, supporting Regional Computer Emergency Response Teams (RCERTs)/Theater Network Operations and Security Centers (TNOSCs), and the Army Computer Emergency Response Team (ACERT). MACOM IAPMs will report to the RCIO of the region in which the headquarters is physically located.

e. Appoint or approve DAAs as required.

f. Establish an oversight mechanism to validate the consistent implementation of IA security policy across their areas of responsibility.

g. Oversee annual security education, training, and awareness programs to all users that address, at a minimum, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering.

h. Oversee the implementation of IA capabilities.

i. Incorporate IA and security as an element of the system life-cycle process.

j. Develop and implement an AUP for all users for privately owned equipment (for example, cell phones, personal digital assistants (PDAs), wireless devices) and ISs prohibited during training exercises, deployments, and tactical operations. Incorporate, as a minimum, the prohibition of utilizing such devices or the limitations of acceptable use, as well as the threat of operational exposure represented by these devices in garrison, pre-deployment staging, tactical, and operational areas.

k. Develop procedures for immediate notification and recall of IA personnel as assigned.

l. Report security violations and incidents to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.

m. Adhere to and implement the procedures of the networthiness certification process.

n. Program, execute, and report management decision packages (MDEPs) MS4X and MX5T resource requirements.

2–8. Commander, 1st Information Operations Command (LAND)

In addition to the responsibilities defined in paragraph 2–2, the Commander, 1st Information Operations Command (1st IO CMD (LAND)) will—

a. Exercise command and control of the ACERT and all of its components (including RCERTs).

b. In coordination with NETCOM/9th ASC, establish tactics, techniques, and procedures (TTPs) for the ACERT, RCERTs, and Local Computer Emergency Response Teams (LCERTs) (if established) as required for computer network operations (CNO).

c. In conjunction with NETCOM, integrate computer emergency response, IA, and CND provider activities into network operations (NETOPS), network management, and information dissemination.

d. In coordination with the DCS, G–3, integrate CND, OPSEC, and INFOCON activities into information operations (IO).

e. Serve as the Army CND provider for security incidents and violations, and in coordination with law enforcement (LE) and counterintelligence (CI) agencies, develop and publish response guidelines, checklists, and procedures.

f. Provide status reports per directives on unusual activities occurring on Army networks worldwide.

g. Support the IA security tool repository and provide recommendations for including new tools.

h. Provide tools, methodologies, procedures, and oversight for the vulnerability assessment program and perform vulnerability assessments through approved programs.

i. Develop and maintain an Army CND vulnerability database for trend analysis.

j. Support and maintain CND through IAVM message staffing, notification, distribution, and resolution.

k. Develop TTPs for a threat warning and notification process.

l. Develop procedures to issue CND lessons learned identified from incidents, intrusions, analyses, or other technical processes.

m. Maintain Army computer network situational intelligence awareness, including network threat analysis and Internet network intelligence.

n. Participate with the CIO/G–6, DCS, G–2, USAINSCOM, NETCOM/9th ASC, and CID in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which IA countermeasures should be directed.

2–9. Commanding General, Network Enterprise Technology Command/9th Army Signal Command

In addition to responsibilities defined in paragraph 2–2 and the MACOM commander responsibilities listed in paragraph 2–7, the Commanding General, Network Enterprise Technology Command/9th Army Signal Command (NETCOM) will—

a. Serve as the DAA for the Army Enterprise, and delegate in writing, as required, DAA responsibilities to regional Installation Management Agency (IMA) Regional Directors, with oversight of any further delegation as required.

b. Operate, manage, monitor, administer, and defend the Army portion of the global information grid (GiG).

c. Perform configuration and patch management for all Army network components and systems.

d. Execute NETOPS missions and functions.

e. Review, coordinate, and evaluate proposed policies, procedures, directives, doctrinal publications, plans, materiel requirements, documents, life-cycle management documents, basis-of-issue plans, and system accreditation documents for all systems fielded, or planned to be fielded, to Army installations as well as similar documents that have implications for adherence to policy.

f. In conjunction with 1st IO CMD, establish TTPs for CNO at all levels that integrate IA/CND provider activities with system and network management and information dissemination.

g. Provide timely flows of NETOPS data to maintain an Attack Sensing and Warning view to all levels.

h. Ensure an operational assessment of IA products is conducted before incorporation into systems under NETCOM management.

i. Maintain a repository of the status and availability of Army critical systems and networks.

j. Manage the DiD security architecture environment, strategies, connections, and configurations against unauthorized access, manipulation, or destruction.

k. Manage the AEI Technical Configuration Control Board (CCB) (when staffed) responsible for the Army security architecture. Establish baseline configuration management guidelines and technical and operational TTPs; and review, approve, prioritize, and manage change to the AEI.

l. Conduct quarterly vulnerability assessments of Top Level Architecture (TLA) critical assets, devices, servers, and IA implemented devices.

m. Participate with the CIO/G–6, DCS, G–2, USAINSCOM, 1st IO CMD (LAND), and CID in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which IA countermeasures should be directed.

2–10. Commanding General, U.S. Army Training and Doctrine Command

In addition to the responsibilities defined in paragraph 2–2 and the MACOM commander responsibilities listed in paragraph 2–7, the Commanding General, U.S. Army Training and Doctrine Command will—

a. Integrate approved IA tools, doctrine, procedures, legalities, and techniques into applicable programs of instruction for TRADOC schools.

b. Develop timely Army-wide IA training literature and training aids, leveraging secure electronic distribution and remote access capabilities.

c. Develop, test, and recommend operational and organizational concepts and doctrine to achieve IA goals.

d. Develop and provide IA requirements to the materiel developers and ensure compliance with AR 381–11 and this regulation.

e. Conduct or participate in operational tests of IA implementations as part of system-wide operational tests, as directed.

f. Integrate IA practices into pre-milestone A activities and events as required.

2–11. Commanding General, U.S. Army Materiel Command

In addition to the responsibilities defined in paragraph 2–2 and the MACOM commander responsibilities listed in paragraph 2–7, the Commanding General, U.S. Army Materiel Command will—

a. Provide Army-wide materiel developer IA support for RDT&E and production.

b. Assist IS functional proponents in identifying security requirements for proposed and existing sustaining base, tactical, and weapons systems.

c. Maintain a repository of tactical IA tools, and distribute tools to fielded tactical systems, as needed. Coordinate with 1st IO CMD to integrate tactical and sustaining-base toolboxes into a seamless repository for Army users.

d. Provide a DA authorized (that is, CSLA) cryptographic advisor to the certification authority (CA) throughout the DITSCAP process.

2–12. Commanding General, U.S. Army Intelligence and Security Command (INSCOM)

In addition to the responsibilities defined in paragraph 2–2 and the MACOM commander responsibilities listed in paragraph 2–7, the Commanding General, U.S. Army Intelligence and Security Command will—

a. Serve as the Army Service Cryptologic Element (SCE) and point of contact for ISs under the purview of the NSA.

b. Provide counterintelligence (CI) support to Army elements on IA matters and advise accreditation authorities on the foreign intelligence threat.

c. Coordinate the C&A for all cryptographic systems and conduct C&A for all Army cryptographic systems at Protection Level 2 (DCID 6/3) and below.

d. Participate with the CIO/G–6, DCS, G–2, 1st IO CMD (LAND), NETCOM/9th ASC, and CID in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which IA countermeasures should be directed.

2–13. Commanding General, U.S. Army Criminal Investigation Command

In addition to the responsibilities defined in paragraph 2–2 and the MACOM commander responsibilities listed in paragraph 2–7, the Commanding General, U.S. Army Criminal Investigation Command (CID) will—

a. Operate the Computer Crime Investigative Unit (CCIU).

b. Conduct criminal investigations involving incidents or intrusions into Army networks and computers.

c. Provide criminal and technical intelligence analyses of vulnerabilities, methodology, tools, techniques, or practices obtained from computer crimes or forensic intrusion analyses to support CND, C&A, and program developers or managers.

d. Participate in IAVA Compliance Verification Team (CVT) inspections.

e. Conduct crime prevention surveys to identify crime-conducive conditions involving U.S. Army networks and systems.

f. Serve as chief enforcer of federal laws governing investigations of networks and systems, serve as the POC for investigation determinations, and interface with federal and civilian LE or investigative agencies.

g. Participate with the CIO/G–6, DCS, G–2, USAINSCOM, NETCOM/9th ASC, and 1st IO CMD (LAND) in analyses and studies concerning foreign intelligence threats, criminal intelligence, or operational vulnerabilities against which IA countermeasures should be directed.

2–14. Program executive officers and program/project managers

In addition to the responsibilities defined in paragraph 2–2 and the MACOM commander responsibilities listed in paragraph 2–7, program executive officers (PEOs) and program/project managers (including PMs outside the PEO structure responsible for fielding systems to multiple Army organizations) will——

a. Acquire, operate, and support systems within their command or activity per this regulation.

b. Embed IA engineering and capabilities in all system RDT&E activities.

c. Appoint an IAPM to perform those duties listed in paragraph 3–2b.

d. Ensure that designated pre-deployment Information Assurance security officers (IASOs) effect continuous coordination with the organizational IA personnel for which the systems are demonstrated, tested, or fielded.

e. Ensure accreditation is submitted to and approved by CIO/G–6 for any system developed for which DAA authority has not previously been delegated by the CIO/G–6.

f. Ensure that the system DAA provides the MACOM, RCIO IAPM, NETCOM, and CIO/G–6 a copy of the draft SSAA 3 months before initial operational test and evaluation (IOT&E) and similarly provides a copy of the approved SSAA before deployment of the system.

g. Integrate IA, COMSEC, and TEMPEST into entire system life-cycle design, development, and deployment. Address and include the addition of any IT/IA personnel (such as system administrator (SA) or network security managers needed to operate the new or expanded system or network) or access requirements and responsibilities for patch management and system administration as part of the development cost of stated system or network.

h. Integrate IA practices into pre-milestone A activities and events.

i. Perform acquisition and life-cycle management of materiel in support of the IA strategy.

j. Report to HQDA CIO/G–6 the percentage of PEO/PM-programmed funding allocated to the AIAP. The report will include current and planned IA investments.

k. Accomplish all intelligence and threat support requirements outlined in AR 381–11 and this regulation.

l. Enforce IA standards per the Joint Technical Architecture Army (JTA–A) and maintain an inventory of IS products, equipment, locations, and contact information.

m. Enact timely IAVM compliance measures (for example, notifications, patch management) and incorporate them into life-cycle management procedures.

n. Ensure cryptographic life-cycle management is a consideration during system design phase.

2–15. Commanders, directors, and managers

In addition to the responsibilities defined in paragraph 2–2 and the MACOM commander responsibilities listed in paragraph 2–7, commanders, directors, and managers (at all levels below the above organizations) responsible for implementing the AIAP in their command or activity will—

a. Acquire, operate, and maintain systems within their command or activity per this regulation.

b. Incorporate and define requests for new systems or changes to existing systems, including security requirements necessary for the system's concept of operation. Once validated, include these security requirements into the system design as defined in procurement contracts. Address the addition of IT/IA personnel (such as SAs or network security managers needed to operate the new or expanded system or network) as part of the development cost of stated system or network.

c. Include IO and IA requirements in submissions of commander's critical information requirements (CCIR) or priority intelligence requirements (PIR).

d. Ensure uses of market-driven/industry-developed (MDID), commercial-off-the-shelf (COTS), or other products are consistent with IA requirements and do not introduce an unacceptable risk.

e. Appoint appropriate IA personnel per chapter 3 of this regulation.

f. Ensure that designated pre-deployment IASOs effect continuous coordination with the organizational IA personnel for which the systems are demonstrated, tested, or fielded.

g. Ensure IA, COMSEC, and TEMPEST requirements are incorporated into life-cycle planning.

2–16. Garrison commanders

In addition to the responsibilities defined in paragraph 2–2 and the MACOM commander responsibilities listed in paragraph 2–7, as applicable, garrison commanders will ensure that the installation-level CCB will provide oversight to—

a. Serve as the DAA for garrison systems and networks.

b. Coordinate with the supporting NETCOM component, MACOM, IMA, and tenant organizations for IA implementation and compliance.

c. Acquire, operate, and maintain systems within their installation or activity per this regulation.

d. Maintain the configuration management of the garrison network.

e. Monitor and manage the connection, access, and IA standards for standalone and networked ISs down to the workstation level across all installation and tenant organizations.

f. Manage and oversee the operation of the installation infrastructure throughout the system life cycle.

g. Provide technical and functional IA guidance and assistance in support of network management.

h. Review, before adoption, proposed changes that could affect the operation of the installation infrastructure's network security and operation (confidentiality, integrity, and availability).

Chapter 3
Army Information Assurance Program Personnel Structure

3–1. Purpose
Commanders will establish an IA personnel structure to implement the AIAP. These personnel will be the focal points for IA matters within their commands or activities and will have the authority to enforce security policies and safeguards for their systems or networks. This authority includes suspending system operations based on an identified security deficiency, poor security practice, or unacceptable risk. Position the IA staff in the organization to ensure that system security is not bypassed at the expense of operations. The IA staff will be involved in the acquisitioning and contracting for ISs or IS services.

3–2. Information Assurance personnel structure
Commanders will position IA personnel organizationally to provide a balance between the security and the operational missions. The following is the AIAP personnel structure and activities to be performed.

a. NETCOM Regional Chief Information Officer (RCIO). NETCOM RCIOs will—

(1) Translate strategic plans and technical guidance provided by NETCOM into objectives, strategies, and architectural guidance.

(2) Exercise staff supervision and technical control for all IT organizations within their region and execute responsibilities for baseline services (communication and system support, visual information, documents management, IA, INFOCON, automation), either operationally or programmatically, as well as oversight of NETOPS.

(3) Provide all personnel operating on Army installations the IT baseline services in a manner consistent with policies and regulations.

(4) Provide administrative, financial, and managerial IT support to any Army post, camp, or station located within their geographic region.

(5) Coordinate the management of outsourced IT services.

(6) Define the baseline and objectives, and establish specific service levels detailing contractual arrangements and satisfactory contractor performance.

(7) Lead enterprise-level initiatives that assure users' training requirements are considered and integrated into processes for developing, implementing, and maintaining capabilities and systems.

(8) Act as the focal point for command, control, communications, and computers for information management (C4IM) leadership and coordination of information technology activities within the region.

(9) Execute the duties assigned under the NETCOM CONOPS for Service Level Agreements, Configuration Management, and Networthiness Certification Program.

(10) Ensure all ISs, networks, and devices are scanned semi-annually as a minimum, including, but not limited to, scanning for vulnerabilities, poor security practices, noncompliance, backdoor connections, unauthorized modems, and unauthorized network connections; take actions to eliminate and report all violations.

(11) Oversee implementation of AIAP policy and procedures within their region.

(12) Oversee the assignment of regional IA personnel and appoint a regional IAPM.

(13) Provide supported MACOMs, organizations, and agencies with POC information, especially if the MACOM is geographically disbursed across several regions.

b. Information Assurance program manager (IAPM). The IAPM will be accountable for establishing, managing, and assessing the effectiveness of all aspects of the IA program within a region, MACOM, or functional activity. A contractor will not fill the IAPM position. (Temporary assignment of contractor personnel for a specified time, as an exception, is authorized until the position can be properly filled.) The IAPM must be a U.S. citizen and hold a U.S. government security clearance and access approval commensurate with the level of responsibility. Designate this position as Information Technology I (IT–I). The IAPM must be IA trained and certified, and maintain the certification. The IAPM will—

(1) Develop, manage, and maintain a formal IA security program that includes defining the IA personnel structure and ensuring the appointment of an Information Assurance network manager (IANM), Information Assurance network officer (IANO), Information Assurance manager (IAM), and an Information Assurance security officer (IASO) at appropriate subordinate command installations, DA staff agencies, tenants, and field operating agencies, as appropriate.

(2) Develop, implement, and enforce Army, regional, or command-unique IA policy.

(3) Ensure that IA personnel review and implement bulletins and advisories that affect the security of their ISs.

(4) Ensure that all IA personnel receive the necessary technical (for example, operating system, network, security management, system administration) and security training to carry out their duties and maintain certifications.

(5) Serve as the primary point of contact for IA-related actions. This includes Information Assurance vulnerability management (IAVM) reporting, compliance, vulnerability assessments, and feedback to Army staff on current and upcoming IA policies.

(6) As applicable, Regional and MACOM IAPMs will provide their supporting RCERT or TNOSC with guidance and priorities regarding IA/CND support to their regions, MACOMs, and subordinates.

(7) Ensure the DITSCAP program is implemented.

(8) Ensure the development of system C&A documentation by reviewing and endorsing such documentation and recommending action to the DAA.

(9) Ensure Army approved procedures are in place for clearing, purging, and releasing system memory, media, output, and devices.

(10) Ensure DAAs maintain a repository for all systems' C&A documentation and modifications.

(11) Ensure that security violations and incidents are reported to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.

(12) Ensure that protective and corrective measures are implemented for vulnerabilities or incidents per direction of the supporting RCERT.

(13) Verify data ownership responsibilities (including accountability, access, and special handling requirements) for each IS or network.

(14) Establish, conduct, and oversee a command program of announced and unannounced IA assessments.

(15) Regional IAPMs will maintain liaison with appropriate Army Theater and DOD activities, at a minimum including CIO/G–6, RCIO, DISA, NSA, the Defense Intelligence Agency (DIA), HQDA, 1st IO CMD, ACERT, supporting RCERT/TNOSC, CID, and INSCOM elements.

(16) Program, manage, execute, and report MDEPs MS4X and MX5T resource requirements.

(17) Administer an IA management control evaluation program separate from, or in support of, Force Protection Assessment Teams (FPATs).

(18) Serve as a member of the configuration management board, where one exists.

(19) In coordination with the DCS, G–3, DCS, G–2, and CIO/G–6, provide technical and non-technical information to support a commander's INFOCON program.

(20) Ensure that program controls are in place to confirm user access requirements.

(21) MACOM/functional IAPMs will ensure that any MACOM-sponsored or developed unique systems are properly accredited and certified. Any proposed distribution will meet networthiness certification and the NETCOM connection approval process, and fulfill all requirements as a standard PM-developed fielding.

c. Regional Information Assurance network manager (IANM). The IANM (if appointed) may serve as the alternate IAPM. A contractor will not fill the IANM position. (Temporary assignment of contractor personnel for a specified period, as an exception is authorized, until the position can be properly filled.) The IANM must be a U.S. citizen and hold a U.S. government security clearance and access approval commensurate with the level of responsibility. This position will be designated IT–I. The IANM must be IA certified and maintain his or her certification. The IANM, under the purview of the IAPM, will—

(1) Provide direct support to the IAPM on matters of CND and the regional/command IA program.

(2) Develop and oversee operational (technical) IA implementation policy and guidelines.

(3) Advise the IAPM or DAA on the use of specific network security mechanisms.

(4) Evaluate threats and vulnerabilities to ascertain the need for additional safeguards.

(5) Assess changes in the network, its operational and support environments, and operational needs that could affect its accreditation.

(6) Ensure procurement actions, installations, and modifications to existing infrastructure comply with Army-approved IA architectural guidance

(7) Develop and staff IA technical policy and procedures for all networks.

(8) Ensure that all networks on the installations or activity for which they are responsible, including tenant networks accessing the host installation's infrastructure, are planned, installed, managed, accredited, maintained, and operated per the security requirements of this regulation and the standards required for connectivity and classification of the network concerned.

(9) Develop and issue network security policy, guidance, and countermeasure implementation instructions to assigned and tenant activities.

(10) Oversee periodic use of authorized scanning and assessment tools.

(11) Assist the IAPM in monitoring and enforcing the IAVM and INFOCON processes.

(12) Serve as a member of the configuration management board, where one exists.

d. Information Assurance manager (IAM). Appoint an IAM at all appropriate levels of command. This includes major subordinate commands (MSCs), posts, installations, and tactical units. Appoint an IAM as needed for those Army activities responsible for project development, deployment, and management of MACOM software, operating systems, and networks. A contractor will not fill the MSC, installation, or post IAM positions and the person filling the position will be a U.S. citizen. Commands, activities, or organizations with multiple IAMs will appoint a senior IAM for their command, activity, or organization. In installations with multiple IAMs, the Installation IAM is the Senior IAM. All IAMs will hold a U.S. government security clearance and access approval commensurate with the level of information processed by the system. This position will be designated IT–I, IT–II, or IT–III. The IAM must be IA trained, certified, and maintain his or her certification. The IAM will—

(1) Develop, maintain, implement, and enforce a formal IA security and training program.

(2) Implement IAVM dissemination, reporting, compliance, and verification procedures.

(3) Report security violations and incidents to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.

(4) Ensure implementation of periodic security inspections, assessments, tests, and reviews.

(5) Manage IASOs, as required, to establish the scope of responsibilities and the technical and security training requirements.

(6) Semi-annually review the status of all ISs and networks to ensure no relevant security changes have been made to invalidate the C&A.

(7) Negotiate C&A issues with the DAA, or his or her designated representative, for incoming systems and make recommendations to the commander on acceptance or rejection of ISs.

(8) Maintain training and certification records for IA personnel and user IA awareness training.

(9) Ensure approved procedures are in place for clearing, purging, destroying, and releasing system memory, media, and devices.

(10) Review all IA C&A support documentation packages and system fielding, operations, or upgrades requirements to ensure accuracy and completeness, and that they meet minimal risk acceptance standards.

(11) Maintain, as required, a repository for all systems C&A documentation and modifications, version control, and management of GOTS, COTS, and non-developmental Items (NDIs) for his or her organization or site.

(12) Establish data ownership and responsibilities (including accountability, access, and special handling requirements) for each IS as required.

(13) Ensure that all ISs within the scope of responsibility are properly certified and accredited in accordance with DITSCAP and configuration management policies and practices before operating or authorizing the use of hardware and software on an IS or network.

(14) Serve as a member of an applicable CCB, where one exists.

(15) Verify that IA personnel are maintaining and auditing access and log data.

(16) Assist the IAPM to identify and validate IA resource requirements.

(17) Provide input to the IAPM for management controls.

(18) The Installation IAM will provide policy and guidance to all IAMs on an installation or cluster of small camps, posts, or stations.

(19) Tenant IAMs will assist and support Installation IAMs.

(20) Installation IAMs will report to the RCIO IAPM.

e. Information Assurance network manager (IANM) or network officer (IANO). The Garrison Commander or manager of the installation or activity responsible for the network will appoint an IANM for each installation or group of networks at all appropriate levels of command below MACOM and DA staff and field operating agencies, including MSCs, posts, installations, and tactical units. Appoint IANOs to assist IANMs as required. IANM and IANO positions will be designated IT–I or IT–II. A contractor will not fill the Installation IANM position. The IANM must be a U.S. citizen and hold a U.S. government security clearance and access approval commensurate with the level of responsibility. Each IANM and IANO must be IA and vulnerability assessment technician (VAT) certified and must maintain his or her certification. The IANM and IANO, in addition to providing direct support to the IAM, will—

(1) Implement the IA program to ensure the AEI is operational and secure.

(2) Comply with and implement policy received from the appropriate network security manager or the IAM.

(3) Document, maintain, and conduct periodic reviews of the network architecture for vulnerability assessments.

(4) Ensure measures and procedures used at network nodes support the security integrity of the network and comply with applicable directives.

(5) Develop, issue, and implement security procedures and protocols governing network operations per this regulation.

(6) Prepare, disseminate, and maintain plans, instructions, and standing operating procedures (SOPs) concerning network security.

(7) Conduct reviews of network threats and vulnerabilities per this regulation and the IAVM process.

(8) Report security violations and incidents to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.

(9) Review and evaluate the effects on security of changes to the network, including interfaces with other networks.

(10) Perform authorized monitoring of network resources per this regulation.

(11) Ensure the use of Army approved IA products per this regulation and AR 380–53.

(12) Implement IA and IAVM reporting and compliance procedures.

(13) Review and maintain network audit data.

(14) Ensure adequate network connectivity by making proper decisions concerning levels of confidentiality and robustness for the system.

f. Information Assurance security officer (IASO). The commander or manager/director of the activity responsible for the ISs will appoint an IASO, as applicable, for each IS or group of ISs. The same IASO may be appointed for multiple ISs. The IASO position will be designated IT–I, IT–II, or IT–III. A contractor may not fill MSC, installation, or post IASO positions if created. The IASO must be IA certified and maintain his or her certification. Appoint pre-deployment or operational IASOs for developmental systems with the applicable responsibilities. DOD uses the term IAO for IASO responsibilities. All IASOs will—

(1) Disseminate and ensure implementation of IA policy, guidance, and training requirements.

(2) Ensure implementation of IAVM dissemination, reporting, and compliance procedures.

(3) Ensure all users meet the requisite favorable security investigations, clearances, authorization, need-to-know, and security responsibilities before granting access to the IS.

(4) Ensure personnel receive system-specific and annual IA awareness training.

(5) Ensure log files and audits are maintained and reviewed for all systems and that authentication (for example, password) policies are audited for compliance.

(6) Prepare, distribute, and maintain plans, instructions, and SOPs concerning system security.

(7) Review and evaluate the effects on security of system changes, including interfaces with other ISs and document all changes.

(8) Ensure that all ISs within their area of responsibility are accredited. Develop or coordinate the development and support of C&A requirements, and initiate re-accreditation as required.

(9) Ensure configuration management for IS software (including IS warning banners) and hardware is maintained and documented.

(10) Ensure system recovery processes are monitored and that security features and procedures are properly restored.

(11) Maintain current software licenses and ensure security related documentation is current and accessible to properly authorized individuals.

(12) Tenant IASOs will support and assist tenant IAMs (or the installation IAM if no tenant IAM exists).

(13) Report security violations and incidents to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.

3–3. Information Assurance support personnel

In addition to the above-described IA structure, other personnel have crucial responsibilities.

a. System or network administrators. System administrators (SAs) and network administrators (NAs) must be designated IT–I, IT–II, or IT–III. Each SA/NA must be trained, experienced, IA certified, and currently certified on the ISs that they are required to maintain. The SA/NA should be a U.S. citizen and must hold a U.S. government security clearance and local access approvals commensurate with the level of information processed on the system or network. SA/NA responsibilities include, but are not limited to, implementing the AIAP within their command, installation, or activity. SA/NAs will—

(1) Implement the IS security guidance policies as provided by the IAM and perform IASO duties if an IASO has not been appointed.

(2) Enforce system access, operation, maintenance, and disposition in accordance with local policies and practices.

(3) Verify that personnel meet required security investigation, clearance, authorization, mission requirement, and supervisory approval before granting access to the IS.

(4) Report security violations and incidents to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.

(5) Perform network scanning and vulnerability assessments with approved software and authorization.

(6) Ensure secure configurations include all pertinent patches and fixes by routinely reviewing vendor sites, bulletins, and notifications and proactively updating systems with fixes, patches, definitions, and service packs with IAM or IAPM approval.

(7) Ensure any system changes resulting from updating or patching are documented with the IASO prior to implementation.

(8) Implement and report IAVM compliance in accordance with locally established policy.

(9) Maintain current anti-virus (AV) engines and definitions on all ISs.

(10) Manage and review user accounts, access, and logins and suspend or terminate accounts in accordance with local policy. Remove inactive accounts that exceed 45 days and departing users' accounts before departure.

(11) Manage, enforce, and audit all account passwords, permissions, inactivity, and suspension policies.

(12) Remove or disable all default, guest, and service accounts in ISs or network devices, and rename administrative accounts as applicable.

(13) Use separate accounts for SA/NA privileged level and general user access.

(14) Review IS and network audit logs and log files, and report anomalous or suspicious information in accordance with Section VIII, Incident and Intrusion Reporting.

(15) Monitor IS performance to ensure that recovery processes, security features, and procedures are properly restored after an IS has been rebooted.

(16) Monitor IS performance to ensure that processes, security features, and operating system configurations are unaltered.

(17) Perform equipment custodian duties as necessary.

(18) Notify the IAM or IAPM when a system no longer processes sensitive or classified information, or when changes occur that might affect C&A, to obtain disposition or resolution instructions.

(19) Ensure configuration management for security-relevant IS software (including IS warning banners) and hardware is maintained and documented.

(20) Implement and test IS and data backup procedures for integrity.

(21) Prohibit attempts to strain or test security mechanisms or to perform network-line or keystroke monitoring without authorization.

(22) Establish audit trails, conduct reviews, and create archives as directed by the IAM.

b. Data owners. Data owners will, at a minimum, provide guidance or feedback to the DAA concerning—

(1) The sensitivity of information under the data owner's purview.

(2) The DAA's decision regarding the level of classification, confidentiality, integrity, availability, and protection requirements for the data at rest or in transit.

(3) Specific requirements for managing the owner's data (for example, incident response, information contamination to other system/media, and unique audit requirements).

(4) Whether foreign nationals may access ISs accredited under this regulation. Access must be consistent with DOD, DA, and DIA governing directives (for example, AR 380–10 and DCIDs 1/7 and 5/6).

c. General users. Users are the foundation of the DiD strategy and their actions affect the most vulnerable portion of the AEI. Users must have a favorable background investigation or hold a security clearance or access approvals commensurate with the level of information processed or available on the system.

(1) User responsibilities.

(a) Comply with the guidelines established under the DOD 5500.7 when making personal use of government-owned ISs.

(b) Participate in annual IA training inclusive of threat identification, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering.

(c) Mark and safeguard files, output products, and storage media per the classification level and disseminate them only to individuals authorized to receive them and with a valid need to know.

(d) Protect ISs and IS peripherals located in their respective areas in accordance with physical security and data protection requirements.

(e) Practice safe network and Internet operating principles and take no actions that threaten the integrity of the system or network.

(f) Safeguard and report any unexpected or unrecognizable output products.

(g) Report the receipt of any media (for example, CD-ROM, floppy disk) received to the IAM or SA, as appropriate, for authorization to use.

(h) Use anti-virus (AV) products on all files, attachments, and media before opening or introducing them into the IS.

(i) Report all known or suspected security incidents, spam, chain letters, and violations of acceptable use to the SA, IAM, or IASO.

(j) Immediately report suspicious, erratic, or anomalous IS operations, and missing or added files, services, or programs to the SA in accordance with local policy and cease operations on the affected IS.

(k) Comply with password or pass-phrase policy directives and protect passwords from disclosure.

(l) Invoke automatic password-protected screen locks on the workstation after not more than 10 minutes of non-use or inactivity.

(m) Logoff ISs at the end of each workday.

(n) Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need to know, and assume only authorized roles and privileges.

(o) Users authorized government-provided IA products (for example, AV or personal firewalls) should be encouraged to install and update these products on their personal systems and may be required to do so as directed by the DAA for any approved remote access.

(2) Prohibited activities. The following activities are specifically prohibited and users will not—

(a) Use ISs for personal commercial gain or illegal activities.

(b) Use ISs in any manner that interferes with official duties, undermines readiness, reflects adversely on the Army, or violates standards of ethical conduct.

(c) Intentionally send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (that is, spam) communications. (LE/CI investigators, attorneys, or other official activities, operating in their official capacities only, may be exempted from this requirement.)

(d) Participate in on-line gambling or other activities inconsistent with public service.

(e) Participate in, install, configure, or use ISs in any commercial or personal DCE (for example, SETI, human genome research).

(f) Release, disclose, or alter information without the consent of the data owner, the original classification authority (OCA) as defined by AR 380–5, the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or disclosure officer's approval.

(g) Attempt to strain, test, circumvent, bypass security mechanisms, or perform network line monitoring or keystroke monitoring.

(h) Modify the system equipment or software, use it in any manner other than its intended purpose, introduce malicious software or code, or add user-configurable or unauthorized software (for example, instant messaging, peer-to-peer applications).

(i) Relocate or change IS equipment or the network connectivity of IS equipment without proper security authorization.

(j) Share personal accounts and passwords or permit the use of remote access capabilities by any individual.

(k) Disable or remove security or protective software or mechanisms and their associated logs.

d. COMSEC custodians and inspecting personnel. Execute responsibilities as required per this regulation and AR 380–40.

e. TEMPEST personnel. Execute responsibilities as required in AR 381–14.

f. Intelligence personnel. Senior intelligence officers (SIOs) or command intelligence officers (DCSINT/G2s/S2s) will—

(1) Ensure the Command Statement of Intelligence Interest (SII) (AR 381–10 and AR 381–20) registers requirements for the receipt of validated intelligence adversely affecting the integrity and reliability of ISs.

(2) Provide assistance in the identification of threat factors affecting the risk management approach for implementing security safeguards.

g. Force protection officers. Execute responsibilities as required by AR 525–13.

h. Information operations officers. Execute responsibilities as required by FM 100–6.

i. Operations security (OPSEC) officers. The primary OPSEC vulnerability is information made publicly accessible through Web sites and Web-enabled applications. Commanders will include an OPSEC review plan as part of their inspection programs. All content placed on a Web site will be reviewed for OPSEC sensitive information. Additionally, execute responsibilities as required per AR 530–1.

j. Public affairs officers (PAOs). Execute IA responsibilities as required per this regulation and AR 25–1.

k. Acquisition officers. Include IA requirements in the acquisition phases and execute responsibilities as required by DOD 5000.2–R and NSTISSP No. 11.

l. Directors of information management (DOIMs). Execute responsibilities per this regulation and AR 25–1.

m. Designated approving authorities (DAAs) (See also para 5–8.)

(1) The DAA will—

(a) Be a U.S. citizen.

(b) Hold a U.S. Government security clearance and access approvals commensurate with the level of information processed by the system under his or her jurisdiction.

(c) Be an employee of the U.S. Government and meet the grade requirements identified in paragraph 5–8.

(d) Ensure the DAA position is designated as an IT–I, based on the duties assigned and the expected effects on the Army mission.

(e) Meet training and certification requirements in accordance with NSTISSI No. 4012–National Training Standard for Designated Approving Authority (DAA), dated August 1997.

(f) The DAA will understand the operational need for the systems and the operational consequences of not operating the systems. The DAA will have an in-depth knowledge of DiD to drive state-of-the-art acquisition, focus a robust training program, and institute executable policy across the IA enterprise.

(2) The DAA will ensure the following as a minimum—

(a) Proper C&A based on systems environment, sensitivity levels, and security safeguards in accordance with this regulation and the DODI 5200.40 (DITSCAP).

(b) Issue written C&A statements (for example, Interim Approval To Operate/Connect (IATO/IATC)), and formal approval to operate (ATO) C&A documentation after formal review of SSAA and C&A documentation.

(c) Maintain records (including use of IA tools) for all IS C&A activities under his or her purview.

(d) Accomplish roles and responsibilities as outlined in this regulation during each phase of the accreditation process and for each IS as required.

(e) Ensure operational IS security policies are in place for each system, project, program, and organization or site for which the DAA has approval authority. MACOM DAAs will approve MACOM specific or unique applications only.

(f) Incorporate security and networthiness (when implemented) as an element of the life-cycle process.

(g) Ensure data owner requirements are met before granting any foreign national access to the system.

(h) Consider and acknowledge CI and criminal intelligence activities during the C&A process.

(i) Report security-related events to affected parties (for example, data owners, all involved DAAs). DAAs must coordinate with investigative activities (for example, CCIU, RCERT) before making notifications.

(j) Assign written security responsibilities to the individuals reporting directly to the DAA (for example, IAM or an IASO if an IAM does not exist).

(k) Appoint a certification agent (CA) for each IS (or group of ISs) and network.

(l) Ensure CSLA certification of cryptographic applications occurs during the C&A process.

n. Certification agent (CA). Each CA must be objective, trained, and experienced on the ISs upon which he or she is required to conduct certification testing. The CA may be Army, DOD, or contractor personnel. Contractors acting in the role of CA will be IT–I or equivalent. When practical, the CA must be an independent and unbiased individual and have a demonstrated understanding of DOD and Army IA policies. The CA must meet training and certification requirements in accordance with NSTISSI No. 4015–National Training Standard for System Certifiers, dated December 2000. Responsibilities include but are not limited to—

(1) Evaluating the technical and non-technical security features for IA C&A.

(2) Ensuring that security testing and evaluation is completed and documented.

(3) Advising the DAA on the use of specific security mechanisms.

(4) Providing C&A documentation to the DAA.

(5) Assessing changes in the system, its environment, and operational needs that could affect the accreditation.

(6) Including CSLA personnel as a cryptographic advisor on certification teams.

o. Host and tenant responsibilities. Army tenant units or activities must comply with the IA requirements of their parent MACOM and the supporting installation. Army and non-Army tenant operations must comply with the host installation's IA policy if they connect to the installation's information infrastructure. Army tenant units or activities and units based in or under operational control (OPCON) of a MACOM other than their parent MACOM will comply with the IA requirements of both parent and host MACOMs. Address unresolved conflicts of IA policy per this regulation through local command channels and NETCOM RCIOs to HQDA, CIO/G–6. Until CIO/G–6 resolves the conflict, the provisions of this regulation will apply, including those pertaining to the use of gateways or information management resources as pathways to connect their ISs. If the non-Army tenant uses any part of the host installation infrastructure, the installation IAM will require the use of configuration management controls consistent with the installation's information management and configuration management process. All tenant activities will—

(1) Identify and coordinate all system upgrades, fieldings, pilots, tests, and operations of new or upgraded systems with the installation IAM, DAA, and DOIM.

(2) Identify ISs and provide the approved C&A documentation to the installation IAM.

(3) Identify their security support requirements to the installation IAM and provide technical assistance, as required.

(4) Identify appropriate IA personnel to the installation IAM.

(5) Support installation IA efforts and requirements, and identify constraints in sufficient time to permit coordination and preparation of a viable IS security solution.

(6) Coordinate and conduct vulnerability assessments or compliance scanning, and report completion and results as required.

Chapter 4
Information Assurance Policy

Section I
General Policy

4–1. Overview

This chapter provides policy to implement IA requirements developed to respond to the IA challenge, or defined in Public Law, National Security, DOD, and Army directives, policies, and regulations.

a. Implement all security analyses, security engineering, and security countermeasures to protect Army ISs within the framework of risk management and adherence to public laws, DOD directives, and Army regulations.

b. Define a security policy and a protection profile for ISs during concept development. Consider security requirements based on these items throughout the IS life cycle.

c. The IS developer will ensure the early and continuous involvement of the functional proponent, threat and risk assessors, users, IA personnel, data owners, certification authorities, and DAAs in defining and implementing security requirements of the IS.

d. Statements of security requirements will be included in the acquisition and procurement specifications and contracts for ISs. Purchases will be in accordance with Army contracting and acquisition, Blanket Purchase Agreements (BPAs), and Army IA-approved products. The statements will reflect an initial risk assessment and will specify the required protection level per DODD 8500.1 and DODI 8500.2.

e. MACOMs, PEOs, PMs, or functional proponents will not field, and installation commanders will not accept, systems—

(1) That do not meet minimum security standards stated in the acquisition and procurement specifications.

(2) For which the DOD or Army DAA does not provide complete documentation supporting C&A.

(3) That have not undergone certification testing and received appropriate accreditation.

f. Commanders are responsible for ensuring that ISs under their purview are operated in a manner consistent with the system C&A and this regulation.

g. Development and modification to existing ISs will be performed in a manner that makes security an integral part of the development, acquisition, fielding, and operational processes.

h. All ISs will be subjected to the Acquisition Life-cycle per AR 70–1.

i. Army Regulation 525–13 prescribes Army antiterrorism and force protection (AT/FP) policy and assigns responsibilities for including defensive information operations into AT/FP Programs.

4–2. Funding

HQDA will manage and provide annual IA initiatives funding guidance and support required for MDEPs MS4X and MX5T, and others as appropriate. Funding guidance will change from year to year, and CIO/G–6 will publish annual guidance on the submission of IA requirements to HQDA and the CIO/G–6 validation processes of those submitted requirements. This funding and budgeting process will continue under the Army Information System Security Program (AISSP) direction and guidance. This annual guidance provided to IAPMs and other appropriate personnel will identify valid IA submission requirements and the type of information required. CIO/G–6 will present validated IA requirements to the appropriate Program Evaluation Group (PEG).

a. Reporting requirements (RCS: CSIM 62). RCIOs and MACOMs will provide the MDEP MS4X Report (illustrated in table 4–1) to the HQDA, CIO/G–6, as indicated below—

(1) Submit FY-phased execution plans to the CIO/G–6 no later than 10 August of each year.

(2) Funded commands must provide a detailed mid-year and year-end actual execution report.

(a) The mid-year actual execution report is due to the CIO/G–6 not later than 10 May of each fiscal year.

(b) The year-end actual execution report is due to the CIO/G–6 not later than 10 October of each fiscal year.

(c) Both the mid-year and year-end actual execution reports must be tied to phased execution plans and reconciled with official Execution Database Summary (218) report.

(d) Review execution reports for unauthorized expenditures and unauthorized fund reprogramming.

(e) HQDA, CIO/G–6 will monitor program execution on a regular basis.

(f) MACOMs receiving management decision package (MDEP) MS4X funds will submit semi-annual reports. (Reporting Requirements (RCS: CSIM–62).)

Table 4––1
MDEP MS4X, Information Assurance Phased Funding Utilization Plan/Actual Execution Report (RCS: CSIM-62) For period ending 092009 (MMYYYY)

Project execution data	Phased Fund Utilization Plan	Estimated cost	Actual obligation	Date obligated	Actual execution
(09/09)	Item (for example, training (what type and number of participants); specific equipment items)	($000)	($000)	($000) (09/08)	Remarks: (for example, status of procurement action, explanation for non-execution of funds in line with execution plan; explain what specific equipment items will be used for)

b. MDEP MX5T funds. MDEP MX5T funds are used in centralized procurement of COMSEC and IA equipment within the Army. The following guidance is provided——

(1) Commanders are responsible for developing their respective MACOM and combatant command-level MX5T requirements. Inputs will be staffed through their local IA channels and provided to the NETCOM RCIO and HQDA for all their sub-activities and subordinate commands.

(2) Garrison commanders and tenant activities will report INFOSEC, COMSEC, and IA requirements to their respective RCIOs.

(3) PEOs are responsible for developing, managing, and providing input to the HQDA for all their PMs.

(4) A PM that reports directly to HQDA is responsible for developing requirements and providing his or her input to HQDA.

(5) Forecast data over a 15-year period for the purpose of short-term, mid-term, and long-term funding projections. Provide this data to the CSLA located at Fort Huachuca, Arizona. Provide the following minimum data——

(a) Name of INFOSEC, COMSEC, or IA system, equipment, or product needed.

(b) Name of system requiring INFOSEC, COMSEC, or IA systems, equipment, or products.

(c) Quantity of each type of INFOSEC, COMSEC, or IA equipment needed starting with the first year of the program objective memorandum (POM).

(d) Name of the approving authority.

(e) Point of contact's name, mailing address, and e-mail and Defense Message System (DMS) addresses.

(f) Name of operational requirements document (ORD) and date approved.

(g) Short description of system.

(h) Other information as directed by HQDA CIO/G–6 or DCS, G–3.

(6) Submission of un-resourced requirements will be to CIO/G–6, Attention: NETCOM ESTA–IAD.

4–3. Information Assurance training

All individuals appointed as IA or network operations personnel must successfully complete an IA security certification course of instruction equivalent to the duties assigned to them.

a. Certification training requirements.

(1) IAPM.

(a) Complete the Army Information Assurance Manager (IAM) Course within 6 months of appointment.

(b) Methods of certification are an Army IAM course, Army E-learning/CBT modules, or other Service or Agency equivalent.

(c) Provide completion date to the compliance-reporting database (CRD) within 2 weeks of course completion.

(2) IANM.

(a) See paragraphs (1)(a) and (c), above.

(b) Complete the SA/NM security course (at Fort Gordon or a mirror site) within 6 months of appointment.

(3) IAM. See paragraphs (1)(a) and (c), above.

(4) IANO. See paragraphs (1)(a) and (c), above.

(5) IASO.

(a) Complete an IASO Course within 6 months of appointment. Methods of training are Web based (http://ia.gordon.army.mil), CD ROM (DISA Operational Information System Security (OISS) CD ROMs), Army E–Learning/CBT IA modules, MACOM (or other Service) course, or the IAM course.

(b) See paragraph (1)(c), above.

(6) SAs.

(a) Complete introductory training (Level I) within 6 months of assuming position. SAs will be certified to Level I as a minimum. Methods include the IASO Course online at Fort Gordon, IAM Course, Army E–Learning/CBT modules, DISA OISS CD ROMs, or the equivalent MACOM or other Service IASO- or IAM-level courses. RCIOs or MACOM IA personnel (as applicable) will determine if limits on SA duties warrant certification to Level I only.

(b) Complete technical training (Level II) 10-day SA Security Course (schedules available at http://ia.gordon.army.mil) or a MACOM-equivalent course within 6 months of assuming position.

(c) Complete advanced training (Level III) at the National Guard Bureau (NGB) Computer Emergency Response Team Operational Training Experience (CERT OTE) or USARC Computer Defense Network Course (CNDC) courses, or other Service or agency equivalents as required.

(d) See paragraph (1)(c), above.

(7) Contracting officer's representatives (CORs). Contracting officer's representatives will compare contractor qualifications to the statement of work requirements to ensure contractor-nominated SA positions meet minimum requirements before acceptance for employment.

(8) IA user training. IAMs, SAs, and IASOs will ensure that a user-training program is in place for all users in the

command. Online user training courses can be found at http://ia.gordon.army.mil. Courses to supplement user training are available through Army E–Learning/CBT.

(a) All users must receive IA awareness training tailored to the system and information accessible before issuance of a password for network access. The training will include the following—

1. Threats, vulnerabilities, and risks associated with the system. This portion will include specific information regarding measures to reduce malicious logic threats, principles of shared risk, external and internal threat concerns, acceptable use, privacy issues, prohibitions on loading unauthorized software or hardware devices, and the requirement for frequent backups.

2. Information security objectives (that is, what needs to be protected).

3. Responsibilities and accountability associated with IA.

4. Information accessibility, handling, and storage considerations.

5. Physical and environmental considerations necessary to protect the system.

6. System data and access controls.

7. Emergency and disaster plans.

8. Authorized systems configuration and associated configuration management requirements.

9. Incident, intrusion, malicious logic, virus, abnormal program, or system response reporting requirements.

10. Information operations condition requirements and definitions.

(b) Users will receive annual refresher training as a minimum or as conditions warrant.

(9) Vulnerability assessment certification. IA personnel conducting vulnerability assessments on Army ISs must achieve VAT certification through their supporting RCERT or TNOSC. (This is not equivalent to the IAVM program assessment procedures.) Additional requirements can be found on the IA BBP Web site.

b. Refresher training. Refresher training for IAPMs, IAMs, IANMs, IASOs, and SAs/NAs will be attendance at an Army IA workshop every 18–24 months, attendance at DOD-sponsored IA workshops, completion of modules in Army E–Learning/CBT IA learning path, or approved commercial courses.

c. Substitutions or equivalencies.

(1) IAPMs, IAMs, IASOs, and IANMs can substitute other Service or Agency courses to fulfill these requirements. Identify the substitute course, duration, and sponsor when tracking completion dates and CRD input.

(2) SAs and IANMs can substitute courses to fulfill the technical training (Level II) requirement.

(3) Substitute coursework must include all topics of the SA Security Course managed by Fort Gordon. For approval of substitute coursework, send an e-mail to CIO/G–6.

(4) Successful completion of the Level III course managed by NGB or the U.S. Army Reserve (USAR) will fulfill Level II certification requirements.

4–4. Mission assurance category, levels of confidentiality, and levels of robustness

a. Mission assurance category. All ISs will be assigned a mission assurance category that reflects the importance of the information relative to the achievement of DOD goals and objectives. The IS mission assurance category will be determined by the DOD or Army proponent. Refer to DODI 8500.2 (http://iase.disa.mil/policy.html) for additional detailed guidance and procedures for defining or assigning mission assurance categories and the BBP when developed for Army applications.

(1) MAC I-high integrity, high availability for DOD ISs handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

(2) MAC II-high integrity, medium availability for DOD ISs handling information that is important to the support of deployed and contingency forces.

(3) MAC III-basic integrity, basic availability for DOD ISs handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term.

b. Levels of confidentiality. All ISs (including interconnected ISs) will be assigned a level of confidentiality (LOC) rating based on the information processed, stored, or transmitted.

(1) High confidentiality for systems processing classified information.

(2) Medium confidentiality for systems processing sensitive information.

(3) Basic confidentiality for systems processing public or unclassified information.

c. Levels of robustness. All ISs will employ protection mechanisms that satisfy criteria for basic, medium, or high levels of robustness per DODI 8500.2 and Federal Information Processing Standard (FIPS) 140–2. Each IS will be managed and operated to achieve the appropriate level of protection for the applicable functional security requirements.

(1) High robustness. High robustness is the security services and mechanisms that provide the most stringent protection and rigorous security countermeasures. Generally, high robustness technical solutions require NSA-certified high-robustness solutions for cryptography, access control and key management, and high assurance security design as specified in NSA-endorsed high robustness protection profiles, where available.

(2) Medium robustness. Medium robustness is security services and mechanisms that provide for layering of

additional safeguards above good commercial practices. Medium robustness technical solutions require, at a minimum, strong (for example, crypto-based) authenticated access control, NSA-approved key management, National Institute of Standards and Technology (NIST) FIPS-validated cryptography, and the assurance properties as specified in NSA-endorsed medium robustness protection profiles or the Protection Profile Consistency Guidance for medium robustness.

(3) Basic robustness. Basic robustness is the security services and mechanisms that equate to best commercial practices. Basic robustness technical solutions require, at a minimum, authenticated access control, NIST-approved key management algorithms, NIST FIPS-validated cryptography, and the assurance properties specified in NSA-endorsed basic robustness protection profiles or the Protection Profile Consistency Guidance for Basic Robustness.

d. Level of total system exposure. The appropriate level of protection for each functional security requirement will be determined using a combination of the mission assurance category and the confidentiality level.

(1) Each IS will be reviewed against the mission assurance category definitions provided in DODI 8500.2, Enclosure 2, and assigned to a mission assurance category.

(2) Each IS will be assigned a confidentiality level based on the classification or sensitivity of the information processed, stored, or transmitted.

(3) Determine the applicable IA controls from DODI 8500.2.

(4) The identified controls for the level of total system exposure serve as the baseline IA requirements for C&A or reaccredidation.

4–5. Minimum Information Assurance requirements

Configure ISs to implement the principle of least privilege through automated or manual means. All risk analyses will evaluate possible vulnerabilities and adverse security effects on the associated ISs and networks within the appropriate areas of responsibility. Although manual procedures are acceptable when an automated safeguard is not feasible, embed automated security safeguards into the design and acquisition of new or updated ISs to ensure a secure infrastructure. Employ technical capabilities to achieve these requirements to the greatest extent possible.

a. Accreditation. Accredit Army ISs in accordance with DODI 5200.40 (DITSCAP), DOD 8510.1–M (DITSCAP Application Manual), and Army supplemental Networthiness guidance (when published).

b. Access control. Implement controls to protect ISs from compromise, unauthorized use or access, and manipulation. IA personnel will immediately report unauthorized accesses or attempts of such systems.

(1) Access to Army ISs or networks is a revocable privilege.

(2) Approval processes will be developed and determined for specific groups and users.

(3) Individuals will meet security investigation (or approved interim access) requirements before IS access.

(4) Systems will automatically generate an auditable record or log entry for each access granted or attempted.

(5) Identify all users through a unique user identification (USERID).

(6) Authenticate user access to all systems with a minimum of a USERID and an authenticator. An authenticator may be something the user knows (password), something the user possesses (token), or a physical characteristic (biometric). The most common authenticator is a password.

(7) Use password-protected screen savers, screen locks, or other lockout features to prevent unauthorized access on all ISs during periods of temporary non-use; configure such mechanisms to automatically activate when a terminal is left unattended for no longer than 10 minutes. Establish a shorter period if appropriate, such as in a multinational work area.

(8) Prohibit anonymous accesses or accounts (for example, Student1, Student2, Patron1, Patron2, anonymous).

(9) The use of group accounts is generally prohibited. Permit exceptions only on a case-by-case basis that support an operational or administrative requirement such as watch-standing or helpdesk accounts, or that permit continuity of operations, functions, or capabilities. IAMs will implement procedures to identify and audit users of group accounts through other operational mechanisms such as a duty logs.

(10) Implement a policy of least privilege for access to system resources or information.

(11) Limit the number of user failed log-on attempts to three before denying access to (locking) that account, when supported by the IS or device. If IS-supported, the system will prevent rapid retries when a password is incorrectly entered and gives no indications or errors that either the password or ID was incorrectly entered (for example, implement time delays between attempts).

(12) A security alert will be generated and investigated when the maximum number of password attempts is exceeded, the maximum number of attempts from one IS is exceeded, or the maximum number of failed log-ins over a period is exceeded.

(13) Reinstate accesses only after the appropriate IA (for example, SA/NA) personnel have verified the reason for failed log-on attempts and have confirmed the access-holder’s identity. Permit automatic account unlocking (for example, established time period elapsed) as an exception only, based on sensitivity of the data or access requirements.

(14) If authorized by the DAA, time-based lockouts (that is, access is restricted based on time or access controls based on IP address, terminal port, or combinations of these) and barriers that require some time to elapse to enable bypassing may be used. In those instances the DAA will specify, as a compensatory measure, the following policies—

(a) Implement mandatory audit trails to record all successful and unsuccessful log-on attempts.

(b) Within 72 hours of any failed log-on and user lockout, IA personnel will verify the reason for failure and implement corrective actions or report the attempted unauthorized access.

(c) The SA will maintain a written record of all reasons for failure for 1 year.

(15) Temporarily disable all accounts for deployed forces on garrison networks unless operationally required.

(16) Prepare procedures for suspending, changing, or deleting accounts and access privileges for deployed forces in the event of capture, loss, or death of personnel having network privilege-level access.

(17) Enable, log, and protect physical access control events (for example, card reader accesses) and audit event logs for physical security violations or access controls to support investigative efforts as required.

c. Remote access (RA).

(1) Any IS being used for remote access will employ host-based security and AV software before authorization to connect to any remote access server.

(2) Encrypt log-in credentials as they traverse the network as required for the level of information being accessed or required for need-to-know separation.

(3) Encrypt all RA for network configuration or management activities regardless of classification level, device, or access method.

(4) Users will protect RA ISs and data consistent with the level of information retrieved during the session.

(5) Disable remote device password save-functions incorporated within software or applications to prevent storage of plain text passwords.

(6) Remote access users will read and sign security and end-user agreements for remote access annually as a condition for continued access.

d. Remote access servers (RASs)

(1) Secure remote terminal devices consistent with the mode of operation and sensitivity of the information and implement non-repudiation measures when necessary.

(2) Any IS that provides RAS capabilities will employ host-based firewalls and intrusion detection systems to detect unauthorized access and to prevent exploitation of network services.

(3) Any RAS being accessed remotely will employ a “Time-Out” protection feature that automatically disconnects the remote device after a predetermined period of inactivity has elapsed, dependant on classification level of the information, but no longer than 10 minutes.

(4) Remote access users will be required to authenticate all dial-in operations with a unique USERID and password, compliant with the remote authentication dial-in user system (RADIUS) standard.

(5) All RAs will terminate at a centrally managed access point located within a DMZ that is configured to log user activities during a session.

(6) Prohibit all RA (that is, VPN, dial-in) to individual ISs within an enclave (that is, behind the DMZ firewall).

(7) DOIMs and IAMs must ensure all RASs undergo CCB and C&A processes.

(8) Stand alone dial-back modems and modem systems that authenticate using RADIUS are the only allowable dial-in modems.

(9) Physical security for the terminal will meet the requirements for storage of data at the highest classification level received at the terminal and must be implemented within a restricted access area.

(10) Approved telework or telecommuting access will be in accordance with established DOIM, RCIO, and NETCOM C&A access procedures from a government provided system only. Ad hoc telework access (defined as one-time, informal, or on an infrequent basis) will be through existing and approved external access methods or portals such as Terminal Server Access Control System (TSACS) or AKO Web site.

(11) Overseas (OCONUS) telework procedures and authorization will be approved by the DAA and RCIO on a case-by-case basis.

(12) Audit all RAS connections at a minimum weekly.

(13) Review RAS devices biweekly for security configuration, patches, updates, and IAVM compliance.

e. Configuration requirements. The following policy will be the minimum used for the configuration management of all systems—

(1) Hardware and software changes to an accredited IS with an established baseline will be effected through the configuration management process.

(2) The CCB or the Configuration Management Board (CMB) for a site must approve modifying or reconfiguring the hardware of any computer system. Hardware will not be connected to any system or network without the express written consent of the IAM and the CMB or CCB. In the absence of a CCB or CMB, the appropriate commander or manager will provide the consent on the advice of the cognizant IA official.

(3) Modifying, installing, or downloading of any software on any computer system may affect system C&A and must be evaluated and approved by the IAM with the local CMB, CCB, and DAA.

(4) ISs must meet minimum levels of total system exposure. See paragraph 4–4 and DODI 8500.2 to establish baseline requirements.

f. Assessments. Commanders will ensure that IA personnel conduct initial and continual assessments (including vulnerabilities), using approved tools, tactics, and techniques to facilitate the risk management process and to ensure compliance with the documented and approved network management, configuration management, IAVM requirements, and security policies and procedures. Commanders and IA personnel will ensure that all networks and networked ISs undergo a self-assessment, vulnerability assessment scan semi-annually. Prohibit the use of commercial scanning services or vendors.

g. Auditing. Log all access attempts. Audits will be either by automated or manual means. Implement embedded or native audit mechanisms for those ISs that support multiple users.

(1) Use audit servers to consolidate system audit logs for centralized review to remove the potential for unauthorized editing or deletion of audit logs in the event of an incident or compromise.

(2) Conduct self-inspections by the respective SA or IA manager.

(3) Enable and refine default IS logging capabilities to identify abnormal or potentially suspicious local or network activity——

(a) Investigate all failed login attempts or account lockouts.

(b) Maintain audit trails in sufficient detail to reconstruct events in determining the causes of compromise and magnitude of damage should a malfunction or a security violation occur.

(c) Retain classified and sensitive IS audit files for 1 year (5 years for SCI systems, depending on storage capability). ACERT, ANOSC, LE, or CI personnel may request IS audit logs to support forensic investigations.

(d) Review logs and audit trails at a minimum weekly, more frequently if required, and take appropriate action.

h. Contingency planning. A contingency plan or COOP is a plan for emergency response, backup operations, transfer of operations, and post-disaster recovery procedures maintained by an activity as a part of its IA security program. Prepare and practice a COOP for each Army IS (a single IS or LAN) as appropriate for critical assets (for example, databases) as identified by the data owner or commander. See DA Pam 25–1–1 for additional guidance and procedures for developing a COOP. Exercise COOP activities annually.

i. Data integrity.

(1) Implement safeguards to detect and minimize unauthorized access and inadvertent, malicious, or non-malicious modification or destruction of data.

(2) Implement safeguards to ensure that security classification levels remain with the transmitted data.

(3) Identify data owners for all ISs. Only the original classification authority (OCA) is authorized to change the data classification.

(4) Implement policies and procedures to routinely or automatically backup, verify, and restore (as required) data, ISs, or devices at every level.

(5) Use data or data sources that have verifiable or trusted information. Examples of trusted sources include, but are not limited to, information published on DOD and Army sites and vendor sites that use verified source code or cryptographic hash values.

(6) Protect data at rest (for example, databases, files) to the classification level of the information with authorized encryption and strict access control measures implemented.

j. System Security Authorization Agreement (SSAA). An SSAA will be maintained by the site-assigned IASO for the life of each IS or LAN, including operational, prototype, test, or developmental systems. This plan will address, as a minimum, the threat, policies, procedures, responsibilities, physical security controls, COMSEC, IA, continuity of operations, and a schedule for implementation and assessment of protection features in accordance with this regulation, DODI 5200.40, or other applicable regulation.

k. IA product acquisition. All security-related COTS hardware, firmware, and software components (excluding cryptographic modules) required to protect ISs will be acquired in accordance with the guidance specified in Public Law 107–314 (*Bob Stump National Defense Authorization Act for Fiscal Year 2003*) and will have been evaluated and validated in accordance with appropriate criteria, schemes, or protection profiles (http://www.niap.nist.gov/) and this regulation. All GOTS products of this nature will be evaluated by NSA or in accordance with NSA-approved processes. NETCOM and CIO/G–6 may approve exceptions to IA products when no criteria, protection profile, or scheme exists or until one is developed, and the removal or prohibition of such IA products would significantly degrade or reduce the ability of IA personnel to manage and protect the infrastructure in the interim.

l. Security training and awareness. All persons accessing an IS will participate in an annual IA security training and awareness program.

m. IS warning banners and labels.

(1) Post appropriate warning banners and labels in accordance with this regulation and AR 380–53.

(2) ISs supporting DOD operations have very specific warning banner requirements, and must include, at a minimum, the information in AR 380–53. The user must take a positive action to accept the terms of the warning banner before a successful logon is completed.

n. Virus protection. Implement the virus protection guidance provided below on all ISs and networks, regardless of classification or purpose—

(1) Scan all files and software, including new “shrink-wrapped” COTS software, with an AV product before introducing them onto an IS or network.

(2) To minimize the risks of viruses, implement the following countermeasures—

(a) Ensure all ISs have a current and supportable version of the AV software configured to provide real-time protection.

(b) Install an AV product for every remote access IS.

(c) IA personnel should take the multilevel approach to virus detection by installing one AV package on the workstations and a different AV package on the servers.

(d) Update virus definitions as a minimum weekly, or as directed by the ACERT for immediate threat reduction. Virus definition availability is based on vendors’ capabilities, and IA personnel will institute processes to automatically update definitions as published or available from authorized DOD or Army sites.

(e) Train users to scan all software, downloaded files, and e-mail attachments to prevent malicious logic installation.

(3) Train users to recognize and report virus symptoms immediately.

(4) IAMs will implement virus-reporting procedures to support DOD and Army reporting requirements.

o. Mobile code.

(1) Mobile code is executable software, transferred across a network, downloaded, and executed on a local system without notification to, or explicit installation and execution by, the recipient.

(2) Mobile code has the potential to severely degrade operations if improperly used or controlled. The objective of the mobile code security policy is to deny untrusted mobile code the ability to traverse the Army enterprise. As a minimum, the Army mobile code mitigation policy will be implemented to support the DOD mobile code policy. Untrusted mobile code will not be allowed to traverse the enterprise unless Army NETCOM CCB-approved mitigating actions have been emplaced. The Army mobile code policy is posted on NETCOM IA Web site.

p. Layering.

(1) Layering is a process of implementing similar security configurations or mechanisms at multiple points in an IS architecture. Doing so eliminates single points of failure, provides redundant capabilities, increases access granularity and auditing, and implements an effective computer or network attack detection and reaction capability.

(2) The Army enterprise IA security DiD structure requires a layering of security policies, procedures, and technological mechanisms protecting all network resources within the enterprise architecture. Layered defenses at the enterprise boundary, for example, include, but are not limited to the following: using proxy services, firewalls, and IDSs, and implementing demilitarized zones (DMZs).

q. Filtering. Filtering policies will block ingress and egress services, sources, destinations, and protocols not required or authorized across the enterprise boundary. Router and firewall ACLs provide a basic level of access control over network connections based on security or operational policy.

(1) Filtering at the enterprise boundary is the primary responsibility of the NETCOM TNOSCs using tools and techniques applied at the TLA network stack.

(2) At all levels subordinate to NETCOM, filtering policies and technology will be layered throughout the architecture and enforced at all capable devices.

(3) Filtering products and techniques will be incorporated, configured, and monitored to reduce security risks to enterprise systems associated with malicious content, misuse, policy violations, threats, or criminal activity without identifying individuals. Examples include, but are not limited to, ACL configuration on routing devices to prevent access to unauthorized sites, AV installations, cache or proxy servers (to maintain connection state), firewalls, mail exchange configurations (for example, auto-deletion of attachments), monitoring software, or IDSs configured to terminate suspicious traffic.

r. Acceptable Use Policy (AUP).

(1) Commanders will develop and publish an AUP for all user accesses under their control. (See the sample AUP at appendix B.)

(2) Users will be advised that there is no expectation of privacy while using Army ISs or accessing Army resources except with respect to LE/CI activities.

(3) Users must review and acknowledge this AUP and IA personnel will maintain documented records.

(4) DOD policy states that Federal Government communication systems and equipment (including Government-owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems), when use of such systems and equipment is paid for by the Federal Government, will be for official use and authorized purposes only.

(5) Official use includes emergency communications and communications necessary to carry out the business of the Federal Government. Official use can also include other use authorized by a theater commander for soldiers and civilian employees deployed for extended periods away from home on official business.

(6) Authorized purposes include brief communications by employees while they are traveling on Government business to notify family members of official transportation or schedule changes. Authorized purposes can also include

limited personal use established by appropriate authorities under the guidelines of the Joint Ethics Regulation (DOD 5500.7–R).

(7) Certain activities are never authorized on Army networks. AUPs will include the following minimums as prohibited. These activities include any personal use of government resources involving: pornography or obscene material (adult or child); copyright infringement (such as the sharing of copyright material by means of peer-to-peer software; gambling; the transmission of chain letters; unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use; or the violation of any statute or regulation.

s. Computer log-on banner. Commanders will ensure that all computers under their control display the Notice and Consent Banner required by AR 380–53 as part of the log on process or access to an IS or device through any service including, but not limited to, ftp, telnet, or other service access. Users must take proactive measures to acknowledge this consent, and user non-consent must prohibit access to the IS or resource (when this capability is supported).

t. Monitoring networks.

(1) Monitoring of networks includes any of a number of actions by IA personnel aimed at ensuring proper performance and management. When any of these monitoring activities involve intercepting (capturing in real time) the contents of wire or electronic communications, they must fall within the limits of the service provider exception to the federal wiretap statute. The service provider exception allows system and network administrators to intercept, use, and disclose intercepted communications as long as the actions are conducted in the normal course of employment and the SA/NA is engaged in an activity that is necessary to keep the service operational or to protect the rights or property of the service provider. Therefore, IA personnel must consult with counsel to ensure that activities involving systems management and protection are properly authorized.

(2) IA individuals performing monitoring activities are authorized to use CIO/G–6-approved automated monitoring tools maintained and configured by NETCOM as network devices to aid in the performance and management. It is important to recognize that the SA/NA does not have unlimited authority in the use of these monitoring tools. The approved tool may contain technical capabilities beyond those tasks for which the tool was approved; as such the IA personnel must ensure that approved tools are used only for their intended purpose. Misuse of automated tools will be reported through appropriate command channels to the Army G6. Exceptions to the configuration of these devices will be approved on a case-by-case basis by the CIO/G–6.

(3) When IA personnel discover information from the normal monitoring activity that indicates a violation of acceptable use or a possible criminal offense, they will immediately report the finding to their commander. The commander will immediately report known or suspected criminal activity to LE and will consult with legal counsel concerning activities that appear merely to violate the AUP. IA personnel will retain and provide information related to the matter to LE.

(4) Only LE/CI personnel are authorized to intercept the content of an individual's communication, after obtaining appropriate legal authority.

(5) Browsing or reading a user's e-mail is prohibited. The SA/NA may intercept, retrieve, or otherwise recover an e-mail message only upon the incident specific consent of the parties involved or as part of a properly authorized LE/CI investigation or as a necessary part of a non-investigatory management search (see para *u,* below). Neither a blanket consent nor the warning banner provides this consent.

(6) The SA/NA may remove any e-mail message or file that is interfering with the operation of an IS without consent of the originator or recipient. The SA/NA will notify the originator and recipient of such actions.

(7) The SA/NA is not authorized to use techniques or software to penetrate or bypass user's information or IS protections (for example, file encryption).

(8) The SA/NA may provide information, facilities, or technical assistance to LE/CI agents if presented with a court order authorizing an interception of communication or a written certification that the emergency provisions of the wiretap statute are being invoked. Assistance to others for the purpose of interceptions is prohibited.

(9) SA/NAs are prohibited from using any automated tools to specifically target an individual user unless the activity is supporting an authorized LE/CI investigation.

u. Management search. In the absence of a user (for example, TDY, extended hospital stay, incapacitation, emergency operational requirement), only the SA/NA is authorized limited access to the user's files to support administrative management searches to provide the requested information as required for official purposes. When such access is requested, the SA will—

(1) Brief the supervisor as to the limits of accessing the user's data files.

(2) Limit the scope of the authorized search to those files reasonably related to the objective of the search (that is, e-mail access would not be reasonable when searching for a word document file).

(3) Limit the search to the time necessary to locate the required data in the most relevant file location.

(4) Inform the individual of requested file access as soon as possible after such requests, and document this access in a memorandum.

(5) SAs/NAs will not grant unrestricted supervisory access to individual information, data files, or accounts.

(6) SA/NAs will not access individual information or data files unless conducting a management search or supporting a LE/CI authorized investigation.

Section II
Software Security

4–6. Controls

a. Implement controls to protect system software from compromise, unauthorized use, or manipulation.

b. The DAA, materiel developer, CIO, or IAM will document and list all software used for control purposes.

c. Software that negates or circumvents system security is prohibited.

d. PEOs, PMs, and functional proponents will require vendors seeking to support the AEI to submit Standard Form 328 (Certificate Pertaining to Foreign Interests).

e. Configuration management controls, including version controls, will be maintained on all software development efforts; research, development, test and evaluation (RDT&E) activities; follow-on test and evaluation (FOT&E) activities; and other related tests by the software designer. A configuration management "baseline image" will be created, documented, kept current (IAVM compliant), and maintained by network and system administration personnel for all ISs within their span of control. Exceptions to this baseline image will be documented. Notify NETCOM RCIOs and the supporting RCERT/TNOSC of local software use approval.

f. The minimum baseline configuration for ISs will be the STIG requirements or the common criteria protection profiles for IA products, as available or supplemented and published by DOD and NETCOM, with changes documented. ISs must meet minimum levels of total system exposure per DODI 8500.2, paragraph 4–4 as part of the baseline requirements.

g. All COTS software used on Army ISs will be fully licensed (under U.S. Copyright Law).

h. Incorporate IAVM compliance, patch management, IA, and AV software into contracts with software developers regardless of the software's purpose (for example, medical devices).

i. Prohibit default installations of "out of the box" configurations of COTS purchased products. COTS purchased products will require system configuration management and IAVM compliance as a minimum. IA products will be on the National Information Assurance Partnership (NIAP) approved products list, or pending certification under an approved protection profile.

j. Systems used or designated as "test platforms" will not remain connected to an operational network. Establish temporary connections to conduct upgrades, download patches, or perform a vulnerability scan, but remove the IS immediately thereafter until it has been operationally accredited and is fully compliant.

k. Use of "shareware" or "freeware" is prohibited unless specifically approved through IA personnel and by the DAA for a specific operational mission requirement and length of time when no approved IA product exists. Notify NETCOM RCIOs and the supporting RCERT/TNOSC of local software use approval.

l. Use of "open source" software (for example, Red Hat Linux) is permitted when the source code is available for examination of malicious content, applicable configuration implementation guidance is available and implemented, a protection profile is in existence, or a risk and vulnerability assessment has been conducted with mitigation strategies implemented with DAA and CCB approval. Notify NETCOM RCIOs and the supporting RCERT/TNOSC of local software use approval.

m. Use of data assurance and integrity products (for example, Tripwire, IPSec, TCP/IP wrappers) should be included in product development and integrated into end-state production systems.

n. IAMs and developers will transition high-risk services such as, but not limited to, ftp or telnet to secure technologies and services such as secure ftp (sftp) and secure shell (ssh).

o. Classified or sensitive information will not be introduced into an IS until the data classification and protection level of the IS has been determined, the appropriate IS protection mechanisms have been put in place, and DAA approval or waiver has been obtained. The data owner will approve entering the data, where applicable. Data will not exceed the security classification level for which the IS has been approved.

p. Upon acceptance for operational use (whether developmental, GOTS, or COTS), keep software under close and continuous configuration management controls to prevent unauthorized changes.

4–7. Database management

a. Databases are the storage for all information and will be managed to ensure that the data is accurate, protected, accessible, and verifiable so that commanders at all levels can rely on trusted information in the decisionmaking process. Commanders will appoint a database administrator (DBA) for each database, as appropriate.

b. The DBA will be certified through either training or experience in the database being managed.

c. The DBA will implement controls to protect database management systems from unauthorized schema modifications.

d. Implement access and auditing controls to protect database management systems from unauthorized accesses and activity.

e. The DBA will conduct weekly backups of the database and schema, as a minimum, or as directed by the IAPM or IAM.

f. Protect databases from direct Internet access using filtering and access control devices (for example, firewalls, routers, ACLs).

g. Data owners will identify the classification or sensitivity of data residing in the database and special controls or access requirements or restrictions for the DBA.

h. Databases will reside on isolated and dedicated servers with restricted access controls. DBAs will not install other vulnerable servers or services (for example, web servers, ftp servers) that may compromise or permit unauthorized access of the database through another critical vulnerability identified in the additional server.

i. Data owners and DBAs will implement and support DOD data/meta-data tagging requirements as initiatives, software, procedures, and methodologies are developed and implemented.

4–8. Design and test

a. All information and information-based systems will incorporate embedded software security solutions throughout the system life cycle.

b. System developers will contact CSLA during initial design to determine COMSEC device requirements (if required) in system design.

c. All information and information-based systems will be tested per an approved Test and Evaluation Master Plan (TEMP) that contains current, validated threats to each IS. The systems will demonstrate successful completion of all required test and evaluation events at each acquisition decision milestone. Conduct vulnerability assessments on all systems before fielding or installing to identify residual vulnerabilities.

Section III
Hardware, Firmware, and Physical Security

4–9. Hardware-based security controls

Consider hardware security, COMSEC, and IA requirements in the concept, design, development, acquisition, fielding, and support of Army ISs.

a. System developers will incorporate controls to protect hardware and firmware from compromise and unauthorized use, removal, access, or manipulation.

b. After initial fielding and installation of hardware or firmware, proposed additions must go through an Installation Configuration Management Control Board for approval before installation and operation. The Configuration Management Board Chair or responsible Information Management (IM) official will notify the DAA, materiel developer, CIO, IAM, NETCOM RCIO, DOIM, or authorized IM officer before installation and operation, as applicable. Proposed additions may require re-accreditation of the system.

c. The C&A will include an inventory of all identifiable hardware, firmware, and software that are parts of the system.

d. Maintain configuration management controls for all hardware and firmware test and evaluation, follow-on test and evaluation, and other related activities by the materiel developer.

e. IAPMs, IAMs, or system developers will contact CSLA to review applicable IA BPAs (both from DOD and the Army) before initiating requisition actions.

4–10. Maintenance personnel

a. Clearances. Maintenance personnel will be cleared to the highest level of data handled by the IS. Clearance requirements should be included in maintenance contracts, statements of work, and specified on the DD Form 254 (Department of Defense Contract Security Classification Specification), in accordance with AR 380–49, where applicable.

b. Restrictions. Escort uncleared maintenance personnel at all times by a cleared and technically qualified individual. Non-U.S. citizens will not perform maintenance on ISs that process TOP SECRET (TS), Sensitive Compartmented Information (SCI), Special Intelligence (SI), Single Integrated Operational Plan-Extremely Sensitive Information (SIOP–ESI), or SAP information.

c. Use of non-U.S. citizens. When non-U.S. citizens are employed to maintain ISs, address such use as a vulnerability in the risk assessment and identify and employ appropriate countermeasures.

d. Maintenance by cleared personnel. Personnel who perform maintenance on classified systems will be cleared and indoctrinated to the highest classification level of information processed on the system. Appropriately cleared maintenance personnel do not require an escort. Need-to-know requirements may be inherent to adequately perform maintenance or take corrective actions. An appropriately cleared and technically knowledgeable employee will be present or review the system during maintenance to assure adherence to security procedures.

e. Maintenance by uncleared (or lower-cleared) personnel. If cleared maintenance personnel are unavailable, individuals with the technical expertise to detect unauthorized modifications will monitor all uncleared maintenance personnel.

(1) Uncleared maintenance personnel will be U.S. citizens. Outside the U.S., where U.S. citizens are not available to perform maintenance, use foreign nationals as an exception, with DAA approval.

(2) Before maintenance by uncleared personnel, the IS will—

(a) Be completely cleared and all nonvolatile data storage media removed or physically disconnected and secured.

(b) When a system cannot be cleared, IAM-approved procedures will be enforced to deny the uncleared individual visual and electronic access to any classified or sensitive information that is contained on the system.

(3) A separate, unclassified copy of the operating system (for example, a specific copy other than the copies used in processing information), including any floppy disks or cassettes that are integral to the operating system, will be used for all maintenance operations performed by uncleared personnel. The copy will be labeled "UNCLASSIFIED–FOR MAINTENANCE ONLY" and protected in accordance with procedures established in the SSAA/System Security Policy (SSP). Ensure that the media is write-protected before use in classified systems.

(4) Maintenance procedures for an IS using a non-removable storage device on which the operating system resides will be considered and approved by the IAM on a case-by-base basis.

(5) IAMs will prohibit the use of commercial data recovery services.

4–11. Security objectives and safeguards

a. Secure removable media that process and store classified information in an area or a container approved for safeguarding classified media per AR 380–5.

b. Establish checks and balances to reduce the risk of one individual adversely affecting system or network operations.

c. Implement physical security requirements for ISs to prevent loss, damage, or unauthorized access.

d. Prohibit storage of portable ISs or personal electronic devices (PEDs) that contain classified information in personal residences. Exceptions will follow the guidance as prescribed in AR 380–5, paragraph 7–6, and authorized as an exception only when an operational requirement exists.

e. Include facilities or spaces housing critical systems (for example, e-mail servers, web servers) as part of the physical security program and restrict access.

Section IV
Procedural Security

4–12. Password control

a. The IAM or designee is responsible for overseeing the password generation, issuance, and control process.

b. The holder of a password is the only authorized user of that password.

c. Change passwords no less frequently than every 90 days (every 30 days if approved password vault software or devices are utilized) and protect them from disclosure.

d. Configure ISs to prevent displaying passwords in the clear unless tactical operations (for example, heads-up displays while an aircraft is in flight) pose risks to life or limb.

e. Generate passwords as follows—

(1) The minimum requirement is a 10-character case-sensitive password. Passwords or phrases longer than 10 characters are recommended when supported by the IS. Password expiration will be not more than 150 days.

(2) The password will be a mix of uppercase letters, lowercase letters, numbers, and special characters, including at least two of each of the four types of characters (for example, x$TloTBn2!) and can be user generated.

(3) Enforce password policy through implementation or enhancement of native security mechanisms.

(4) Passwords will not include such references as social security numbers (SSNs), birthdays, USERIDs, names, slang, military acronyms, call signs, dictionary words, consecutive or repetitive characters, system identification, or names; neither will they be easy to guess (for example, mypassword, abcde12345).

(5) Password history configurations will prevent reutilization of the last 10 passwords when technically possible.

f. IAMs-will approve and manage procedures to audit password files and user accounts for weak passwords, inactivity, and change history. Conduct quarterly auditing of password files on a stand-alone, secured system with limited access. Encrypt password files for transit if auditing at a centralized location.

g. Deployed and tactical systems with limited data input capabilities will incorporate password control measures to the extent possible.

h. Implement other authentication techniques (for example, biometrics, access control devices, or smart cards) as viable alternatives in conjunction with, or in place of, passwords as tested or approved by NETCOM and CIO/G–6.

i. Remove or change default, system, factory installed, function-key embedded, or maintenance passwords.

j. Prohibit automated scripts or linkage capabilities, including, but not limited to, Web site links that embed both account and authentication within the link.

k. SAs/NAs will implement procedures for user authentication or verification before resetting passwords or unlocking accounts.

l. The use of password generating software or devices is authorized as a memory aid when it randomly generates and enforces password length, configuration, and expiration requirements; protects from unauthorized disclosure through authentication or access controls; and presents a minimal or acceptable risk level in its use.

4–13. Release of information regarding information system infrastructure architecture

a. Protect and restrict access to all documentation (for example, maps, test and evaluation results, vulnerability assessments, audits, results, or findings) describing operational IS architectures, designs, configurations, vulnerabilities, address listings, or user information. This information is a minimum of FOUO and will not be made publicly accessible. Evaluate Freedom of Information Act (FOIA) requests for such documents in these categories on a case-by-case basis. Coordinate with your servicing FOIA or Privacy Act office and servicing judge advocate or legal advisor before releasing or deciding to withhold such documents.

b. All information or IS responses that document or display specific vulnerabilities of a system or network that would aid attempts by an adversary to compromise those critical systems or networks are OPSEC sensitive and will be protected, controlled, marked, or stored at the appropriate classification level for the system concerned. This information will not be made publicly available.

c. Protect and restrict access to information that is a collection of interrelated processes, systems, and networks that provides information on IA services throughout the Army; the KMI; or the incident detection and response infrastructure, capabilities, or configuration. This information is a minimum of FOUO and is exempt from the Freedom of Information Act (exemption category 2).

Section V
Personnel Security

4–14. Personnel security standards

The following standards designate positions requiring access to information technology (IT) and for processing information within IT systems. These security designations are required to distinguish potential adverse effects on Army functions and operations and, therefore, the relative sensitivity of functions performed by individuals having certain IT privileges. These positions are referred to as IT and IT-related positions. The requirements of this section will be applied to all IT and IT-related positions, whether occupied by DA civilian employees, military personnel, consultants, contractor personnel, or others affiliated with the DOD (for example, volunteers). Additional guidance is available in DOD 5200.2–R.

a. Basic requirements. Personnel requiring access to ISs processing classified information to fulfill their duties will possess the required favorable security investigation, security clearance, formal access approval, and need-to-know.

(1) IT–I.

(a) Defined as personnel in IA positions (for example, SAs/NAs for infrastructure devices, IDSs, routers; SAs/NAs for classified systems and devices) with privileged-level access to control, manage, or configure IA tools or devices, individual ISs, networks, devices, and enclaves.

(b) Favorable completion of a National Agency Check (NAC) (current within 180 days).

(c) Initiation of a Single Scope Background Investigation (SSBI) or favorable review of SF85P, SF 86, and Supplemental Questionnaire.

(2) IT–II.

(a) Defined as personnel in IA positions (for example, operating system administration of common applications or enclaves, back-up operators) with limited privileged-level access to control, manage, or configure ISs and devices.

(b) A favorable review of local personnel, base/military, medical, and other security records as appropriate.

(c) Initiation of a National Agency Check with Credit Check and Written Inquiries (NACIC) (for civilians) or a National Agency Check with Local Agency and Credit Checks (NACLC) (for military and contractors), as appropriate or favorable review of SF85P and Supplemental Questionnaire.

(3) IT–III.

(a) Defined as personnel in IA positions (for example, normal users, power user on individual systems for configuration) with non-privileged level access to ISs and devices.

(b) A favorable review of local personnel, base and military, medical, and other security records, as appropriate.

(c) Initiation of a NACIC (for civilians) or NAC (for military and contractors), as appropriate or favorable review of SF85P and Supplemental Questionnaire.

b. Personnel security controls.

(1) Personnel security controls, both technical and non-technical (for example, separation of duties, least privilege, identification and authentication (I&A), digital signatures, and audits), will be incorporated into the IS and IS procedures, as appropriate.

(2) Individuals assigned to IT–I, IT–II, or IT–III positions who lose their clearance or have access to classified

systems suspended pending the results of an investigation will be barred access to ISs until favorable adjudication of that investigation. Waivers for access to unclassified systems will be justified in a written request, with the commander's concurrence, to the DAA for approval. Access will be granted only upon DAA signature. Waivers can be processed for IT–II and III personnel only, and are valid for a period not to exceed 6 months. Users designated in IT–I positions will be removed from these positions and access is non-waiverable for IT–I positions.

c. Access by non-U.S. citizens.

(1) Minimize employment of non-U.S. citizens in IT positions. However, compelling reasons may exist to grant access to DOD IT resources in those circumstances in which a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed for a specific DOD requirement and for which a suitable U.S. citizen is not available.

(2) Access to sensitive information by a non-U.S. citizen who is not a DOD employee will only be permitted in accordance with applicable disclosure policies (for example, National Disclosure Policy 1, DODD 5230.9, DODD 5230.25) and U.S statutes (for example, the Arms Export Control Act, 22 USC 39).

(3) If information to which the incumbent will have access is authorized for foreign disclosure, non-U.S. citizens assigned to DOD IT positions are subject to the investigative requirements outlined below.

(4) Non-U.S. citizens may hold IT positions under the conditions described in the paragraphs below and if the DAA that accredited the system and the data owners approve the assignment requirements in writing. The written approval must be on file before requesting the required investigation. The required investigation must be completed and favorably adjudicated before authorizing access to DOD systems or networks. Interim access is prohibited.

(5) The required investigation levels for an IT–I position are outlined below in table 4–2.

Table 4–2
Investigative levels for users with privileged access (IT–I) to ISs

Privileged access—IT–I[1]					
User roles	**Foreign national**	**U.S. civilian**	**U.S. military**	**U.S. contractor**	**Conditions or examples**
DAA or IAPM	Not allowed	SSBI	SSBI	Not allowed	None
IANM	Not allowed	SSBI	SSBI	Conditional SSBI	With CIO/G–6 written approval, contractors may continue as IA personnel until replaced
IAM	Not allowed	SSBI	SSBI	Conditional SSBI	Contractor may not fill MSC, installation, or post IAM position
IASO/IANO	Not allowed	SSBI	SSBI	Conditional SSBI	Contractor may not fill MSC, installation, or post IASO/IANO position (if created)
Monitoring or testing	Not allowed	SSBI	SSBI	SSBI	None
SA/NA or Administrator (with IA administrative privileges) or maintenance of IA devices	Conditionally allowed—SSBI (equivalent)[2]	SSBI	SSBI	SSBI	Examples: administration of IA devices (e.g., boundary devices, IDSs, routers, and switches)

Notes:
[1] Investigative levels are defined in DOD 5200.2–R. The term Foreign National (FN) refers to all individuals who are non-U.S. citizens, including U.S. military personnel, DOD civilian employees, and contractors.
[2] FN—under the immediate supervision of a U.S. citizen with written approval of CIO/G–6.

(6) The required investigations levels for an IT–II position are outlined below in table 4–3.

Table 4–3
Investigative levels for users with limited privileged access (IT–II) to ISs

Limited privileged access—IT–II[1]					
User roles	FN (see note 2)	U.S. civilian	U.S. military	U.S. contractor	Conditions or examples
IAM/IANM (with no IA administrative privileges)	Not allowed	NACI	NACLC	NACLC	None
IANO/IASO (with no IA administrative privileges)	Conditionally allowed—NACLC equivalent	NACIC	NACLC	NACLC	FN—with DAA written approval, direct or indirect hires may continue as IA personnel until they are replaced, provided they serve under the immediate supervision of a U.S. citizen IAM and have no supervisory duties
Supervisor of IT positions	Not allowed	NACI	NACLC	NACLC	None
Administrator (with no IA administrative privileges) or maintenance of IA-enabled products	Conditionally allowed—NACLC equivalent[2]	NACI	NACLC	NACLC	Examples: IS administration, OS administration, end-user administration, and administration of common applications (e.g., e-mail, word processing)

Notes:

[1] Investigative levels are defined in DOD 5200.2–R. The term Foreign National (FN) refers to all individuals who are non-U.S. citizens, including U.S. military personnel, DOD civilian employees, and contractors.

[2] FN—under the immediate supervisor of a U.S. citizen.

(7) Assignment (including assignments due to accretion of duties) of current DOD employees, military personnel, consultants, and contractors to positions with different responsibilities or changed access privileges requires verification of the appropriate investigative basis and authority for holding a position of that level of sensitivity.

d. Interim assignments.

(1) Individuals–excluding non-U.S. citizens but including temporary, intermittent, or seasonal personnel–-may be assigned to unclassified IT–I, IT–II, and IT–III positions on an interim basis before a favorable completion of the required personnel security investigation only after the conditions specified have been met. Interim access is not authorized for non-U.S. citizens.

(2) The security manager at the requesting activity will make interim assignment approvals for civilian and military personnel. The government sponsor's security manager or official will make the approval for contractor or volunteer access.

e. Adjudication.

(1) The provisions of this section apply only to contractor personnel. (Civilian employees, military personnel, consultants, volunteers, and seasonal, part-time, and intermittent employees will be favorably adjudicated by the appropriate DOD central adjudication facility.)

(2) OPM will adjudicate investigations for a trustworthiness determination using the national adjudicative guidelines for access to classified information. If the adjudication is favorable, OPM will issue a letter of trustworthiness to the requesting activity.

(3) If a favorable trustworthiness is indeterminate, OPM will forward the case to the Defense Office of Hearings and Appeals (DOHA) in Columbus, OH, for further processing under DODD 5220.6. A final unfavorable decision precludes assignment to an IT–I, II, or III position.

(4) Enter all OPM IT trustworthiness determinations of DOD contractor personnel into the OPM Security/Suitability Investigative Index (SII).

f. Reinvestigation. Individuals occupying an IT position will be subject to a periodic reinvestigation according to prevailing policy.

4–15. Foreign access to information systems

a. To ensure standardized and appropriate access to the Unclassified but Sensitive Internet Protocol Routing Network (NIPRNET) by foreign officials, IA personnel will meet the requirements delineated below. Provide each authorized foreign official a .mil address on the unclassified network required for executing his or her foreign national duties as outlined in his or her respective certification. For each authorized foreign official, the local area network administrator will place a caveat or marker on all outgoing e-mails from that person identifying him or her as a foreign official from a specific country. In doing so, the local area network administrator will spell out the words "Foreign Official" and the country name of the foreign official and will not use an acronym for that country. In addition, the local area administrator will indicate the type of foreign official access that is granted. The required tags for each of the five categories of foreign officials would thus read as shown below (replace each hypothetical country name with the appropriate one).

(1) Foreign liaison officer (FLO): “Last Name, First Name Middle Initial-Foreign National-Germany-FLO.” (Note: Local area network administrators will designate FLOs representing the United Kingdom, Canada, or Australia as STANREPs rather than as FLOs.)

(2) Cooperative Program Personnel (CPP): “Last Name, First Name Middle Initial-Foreign National-Turkey-CPP”.

(3) Engineer and Scientist Exchange Program (ESEP): “Last Name, First Name Middle Initial-Foreign National-Israel-ESEP”.

(4) Standardization representative (STANREP): “Last Name, First Name Middle Initial-Foreign National-United Kingdom-STANREP”.

(5) Military Personnel Exchange Program (MPEP): “Last Name, First Name Middle Initial-Foreign National-Italy-MPEP”.

b. Limit access to foreign officials, exchange personnel, or representatives to computers that incorporate Army-mandated access and auditing controls. Approval to access the NIPRNET does not equate to authority to exchange data or access systems located on that network. The appropriate system DAA will approve access to foreign nationals on an as needed basis. Similarly, the designated release or disclosure authority will grant access to the information on ISs to foreign officials on an as-needed basis.

c. E-mail signature blocks will be automatically generated for all foreign officials, and include the foreign individual’s nationality and position.

d. If the organization where a foreign official is certified determines there is a need for the foreign official to have access to the NIPRNET beyond e-mail access (for example, an AKO account), submit an exception to policy through the DAA to the RCIO IAPM, to be forwarded to the HQDA CIO/G–6. The exception will be reviewed by the DCS, G–2 Foreign Disclosure Directorate prior to disposition. The exception must include the following information——

(1) Request from the commander that states the need to know tied to the foreign official’s certification and Delegation of Disclosure Authority Letter (DDL).

(2) Statements from the installation and command’s IAM stating proper security procedures are in place. The exception will also be reviewed by the DCS, G–2, Foreign Disclosure and Security Directorate before disposition.

e. Official access to information residing on an IS or network will be limited to that controlled but unclassified information required to fulfill the terms of the contract or agreement provided minimum security requirements of this section are met.

f. Disclosure of classified military information to foreign governments and international organizations is limited and will be in accordance with AR 380–10, DOD Directive 5230.11, and CJCSI 5221.01.

g. NIPRNET access policy and procedures for foreign nationals, defined as personnel in non-official positions, are as follows——

(1) Components or organizations will maintain records on access including the following information—

(a) Specific mission requirements for foreign access or connection.

(b) Justification for each individual foreign national.

(c) Confirmation that the minimum-security requirements of this section are enacted, including the user agreement.

(d) Requesting command or organization POC.

(2) Before authorizing foreign national access to a specific IS on the NIPRNET or the Secret Internet Protocol Routing Network (SIPRNET), Army components will—

(a) Ensure the information is properly processed for disclosure.

(b) Ensure DAAs and data owners concur with the access.

(c) Ensure the C&A documentation for the system is updated to reflect foreign national access.

(d) Ensure security measures employed adhere to this policy.

(e) Validate the identity of each foreign national authorized access to ISs to ensure accountability of all actions taken by the foreign user.

(f) Ensure the foreign national follows appropriate security policies and procedures and that the IASO possesses the authority to enforce these policies and procedures. Before accessing any system, a foreign national will sign a user agreement that includes—

1. Acknowledgment of appropriate information security policies, procedures, and responsibilities.

2. The consequences of not adhering to security procedures and responsibilities.

3. Identification requirements when dealing with others through oral, written, and electronic communications, such as e-mail.

4. Department of the Army employees or contractors who are foreign nationals and are direct or indirect hires, currently appointed in IA positions, may continue in these positions provided they satisfy the provisions of paragraph 4–14, DODD 8500.1, DODI 8500.2, and DOD 5200.2–R; are under the supervision of an IAM who is a U.S. citizen; and are approved in writing by the DAA.

5. Foreign nationals assigned into IT positions will be subject to the same (or equivalent) vetting as U.S. citizens.

6. Foreign nationals may hold or be authorized access to IT–II and IT–III positions provided the required background investigation has been completed or favorably adjudicated.

7. Additionally, a foreign national may be assigned to an IT–I position only after the DAA who owns the system and the data owner who owns the information sign a waiver and the assignment has been approved by the CIO/G–6. Sign and place the waiver in the individual's security file before requesting the required background investigation. The required background investigation must be completed and favorably adjudicated before authorizing IT–I access to DA systems/networks.

8. Do not assign foreign nationals to IT–I, IT–II, or IT–III positions on an interim basis before a favorable adjudication of the required personnel security investigation.

h. Generally, a foreign national or official representative is not authorized access to the U.S. controlled SIPRNET terminal workspace. If an authorized foreign official or national working at a U.S. Army site has a requirement for accessing the SIPRNET, the commander will submit an exception to policy through the DAA to the RCIO IAPM, to be forwarded to the HQDA CIO/G–6, and reviewed by the DCS, G–2 Foreign Disclosure Directorate prior to disposition. CIO/G–6 will coordinate the request with the Army staff and forward to DISA and these requests will be staffed with the presumption of denial. Apply the procedures of this section after DISA's approval and any additional guidance provided by DISA on the connection process for foreign nationals. E-mail signature blocks will be automatically generated for all foreign nationals, and include the foreign individual's nationality and position.

Section VI
Information Systems Media

4–16. Protection requirements

a. All IS equipment and facilities used for processing, handling, and storing classified data will be operated and secured per the DCID 6/3, AR 380–5, this regulation, or Joint DODIIS Cryptologic SCI Information Systems Security Standards (JDCSISSS).

b. Media will be classified, declassified, marked, released, shipped, stored, processed, and transmitted per this and other applicable regulations.

c. Control ISs containing non-removable, non-volatile media used for processing classified information.

d. Commanders and IA personnel will plan, prepare, and train users, administrators, and security personnel in processes for accidental or incidental procedures of spillage of higher-level classified information to a lower-level IS.

e. Configure ISs to apply security or handling markings automatically when possible or available.

f. Configure ISs to display the classification level on the desktop or login screen (for example, wallpaper, splash screen) when locked or logged off.

g. Employees will not transmit classified information over any communication system unless using approved security procedures and practices (that is, encryption, secure networks, secure workstations, and ISs accredited at the appropriate classification level).

4–17. Labeling, marking, and controlling media

a. Unless write-protected or read-only, classify media inserted into a system at the highest level the system is accredited to process until the data or media is reviewed and validated by the IASO.

b. Clear media before reuse in ISs operating at the same protection level.

c. Mark and control all media devices, peripherals, and ISs per this regulation and supplemented as follows:

(1) TS or SCI or intelligence data per DCID 6/3, DCID 1/7, AR 380–5, and JDCSISSS as applicable.

(2) Classified media per AR 380–5.

(3) FOUO media per AR 25–55.

(4) Privacy Act media (sensitive) as FOUO per AR 340–21.

(5) NATO information per AR 380–15.

d. Mark and control the media or IS after determination of the classification level of the data placed on the media. Implement media accountability procedures based on the classification of the data.

4–18. Clearing, purging (sanitizing), destroying, or disposing of media

a. Procedures for disposition of unclassified hard-drive media outside DOD custody will follow current DOD guidelines and additional guidance will be addressed in a Disposition of Hard Drives BBP.

b. Clear media for reuse within the same organization at the same or higher classification level (for example, moving unclassified hard drive to classified network).

c. Purge media before release to or use by another DOD organization for reuse at the same or higher classification level (for example, NIPRNET–NIPRNET or SIPRNET–SIPRNET or NIPRNET–SIPRNET) and ensure equipment transfer custodial requirements are accomplished. Purging does not declassify the media.

d. Purge unclassified media before consideration for release outside DOD control.

e. Destroy media that has ever contained NSA Type 1 cryptographic or COMSEC materiel.

f. Destroy SCI media.

g. Destroy media that contained classified materiel or was involved in a classified spillage incident at end of life cycle.

h. When it is more cost effective, destroy media instead of purging or declassifying.

i. The IAM will establish procedures to periodically verify the results of any purging and IS release processes.

j. Spillage of higher-classified information to lower-classified systems is addressed in published BBPs.

Section VII
Network Security

4–19. Cross-domain security interoperability

The DOD Global Information Grid, Inter-connection Approval Process (GIAP) was created out of the need to provide a consistent way to simplify and consolidate the various connection approval processes. All DOD Services and agencies must comply with these processes when connecting networks of different classification levels. The Top Secret and Below (TABI) and the Secret and Below Interoperability (SABI) processes provide an integrated, comprehensive, and consistent approach to addressing the shared risk associated with the connection of networks of different classification levels.

a. Organizations requiring a cross-domain solution must first complete the information on the GIAP Web site (http://giap.disa.smil.mil).

b. Organizations requiring a cross-domain solution will also contact the NETCOM Information Assurance Directorate, Cross-Domain Solutions Office to provide notification of the cross-domain process initiation.

c. The cross-domain process follows the four phases of the DITSCAP and requires that networks be fully certified and accredited and that all associated security devices be certified, tested, and evaluated (CT&E) in accordance with the NSA compliance standards. Approved standardized cross-domain solutions will be acquired through CSLA. Non-standard solutions will require an extensive engineering effort.

d. All Army organizations that maintain connections between networks of different classification levels must annually revalidate their connections in accordance with the SIPRNET DAA directives. Contact the SIPRNET Connection Approval Office for current guidance and requirements.

e. Manage all interconnections of DOD ISs to continuously minimize community risk by ensuring that one system is not undermined by vulnerabilities of other interconnected systems and that one system does not undermine other systems. All ISs within interconnected (or trusted networks) will meet networthiness certification.

f. Additional or specific implementation measures will be addressed in a BBP once identified.

4–20. Network security

a. Procedures. Establish procedures to manage and control access to all ISs, networks, and network equipment to ensure integrity, confidentiality, availability, non-repudiation, and authentication, regardless of classification level.

b. Requirements. Positive IA measures ensure all users satisfy the requirements specified before granting an individual access (including dial-up services and Internet access) to DOD and Army networks, systems, and stand-alone computers.

(1) Individual. Deny physical and logical access to individuals who cannot meet access requirements.

(2) Proponents. Proponents for programs that require unofficial network services for dependents, retirees, and other individuals serviced at Army installations (for example, morale, welfare, and recreation; libraries; education centers; Army-Air Force Exchange Service (AAFES)) should arrange for service by a commercial Internet service provider (ISP). Proponents will coordinate with the installation DOIM for service and the IAM for IA requirements. These connections are for unofficial communications and are prohibited from connecting to DOD or Army network.

(3) Joint inter-agency and multinational (JIM) networks. JIM networks that have NETCOM-provided connectivity will implement the most restrictive and isolating configuration and implementation management principles (inclusive of, but not limited to, separate enclaves and identifications, and tunneled or dedicated connectivity) to those that are absolutely required for military or support operations as necessary and in compliance with IA requirements in this and other applicable regulations.

c. Restrictions. Users, supervisors, and managers will—

(1) Ensure transmission of classified or sensitive information via applicable secure means.

(2) Authorize commercial ISP accounts per chapter 6, AR 25–1.

(3) Prohibit cross-connections directly between the Internet and NIPRNET of ISs. For example do not permit a modem (for example, copier/fax/printer combinations) connection to a commercial ISP or service while the IS is also connected to the NIPRNET.

(4) Permit direct connections to the Internet to support electronic commerce when those systems will not connect to the NIPRNET or the SIPRNET.

d. Security protection between enclaves (that portion of the network outside the installation's or activity's controls). Utilize the following processes on routers, switches, firewalls, and other networking devices to provide protection from external networks.

(1) Firewalls. Utilize and configure firewalls with least-privilege access controls. Layer firewalls at the boundaries between border and external networks and as needed throughout the architecture to improve the level of assurance. NETCOM will approve firewall implementation guidance for use within the Army.

(2) Access control lists. Access control lists (ACLs) will be used and updated through secure mechanisms and will incorporate a "deny all, permit by exception" policy enforcement.

(3) Network configurations. IA personnel will implement network configurations to remove or block any unnecessary or unauthorized services, software, and applications (for example, LanMan, gaming software, Gnutella, IRC, ICQ, Instant Messaging, peer-to-peer).

(4) Ports, protocols, and services (PPSs). Permit only ports, protocols, and services as authorized by applicable authority.

(a) Army Enterprise and Enclave boundary firewalls and firewall-like devices will restrict the usage of ports, protocols, and services in accordance with BBPs as compiled by the DOD Ports, Protocols, and Services (PPS) Technical Advisory Group (TAG). The DOD TAG PPS list is posted on the Army IA Web site. DOD considers PPSs not listed on the DOD PPS TAG list as "deny by default."

(b) PPSs designated as "high-risk" are unacceptable for routine use. Prohibit high-risk PPSs unless expressly approved for a specific implementation with defined conditions and risk mitigation strategies.

(c) PPSs designated as "medium-risk" have an acceptable level of risk for routine use when used with required mitigation strategies.

(d) PPSs designated as "low-risk" are recommended as best security practices and advocated for use by Army developers in future systems and applications. Not all low-risk PPSs are acceptable under all implementations and may require approval.

(e) The goal of NETCOM is to migrate systems that use high- and medium-risk PPSs to low-risk PPSs as part of its life-cycle management processes through system redesign while maintaining current standards-based applications and requirements (for example, port 21 for ftp, port 80 for Web).

(f) NETCOM is responsible for PPS management and will approve and publish Army-wide mitigation strategies for PPSs.

(5) Domain name service (DNS). TNOSCs will monitor DNS servers for compliance and adherence to DNS policies. Owning organizations will provide host-based intrusion detection monitoring for these servers.

(6) Virtual private networks (VPNs). Virtual private networks will require approval to connect and operate from the RCIO using NETCOM CCB-approved and published implementation processes (when implemented) after documenting a well-defined acceptable use policy, security concept of operations, and an SSAA risk analysis and management plan, before implementation.

(7) Storage area configurations. As developing technologies (for example, storage area networks, collaborative environments, data sharing technologies, webcasting, or real/near-real time distribution capabilities) are implemented, they must incorporate secure IA principles. Minimum requirements include, but are not limited to, the following—

(a) Approved by RCIOs using NETCOM configuration-management approved and published implementation processes (when implemented).

(b) Secure the information at rest or in transit and ensure it will not introduce additional risks or vulnerabilities.

(c) Must support secure communication and access protocols.

(d) Must implement security controls and validate all user supplied input.

(e) Extranet connections will implement a multi-tiered and layered approach requiring separate and distinct servers across the environment for each tier, and minimally include—

1. User access tier, usually through a Web site that offers static pages and will be SSL enabled as a minimum.

2. Application tier, authenticates authorized users, access, and interfaces between the user and the data.

3. Protection of the database or data tier (for example, flat files, e-mail), information that is accessed by the application on behalf of the user.

(f) Incorporate firewalls, filtering, and monitoring devices (for example, IDSs) before and between each layer.

(g) Should employ encryption, single-sign-on, tokens, or digital certificates equivalent to the level of data accessed or available and adequately passed through the application server to access the data requested.

(h) Data tier architecture or IS should employ data separation and authentication "need to know" measures and requirements.

e. Protection of internal networks (portion of the network that is directly controlled by the installation or activity).

(1) Establish trusts in accordance with the installation C&A. There will be no trusted relationships established with any other domains or networks until both are networthiness certified (when implemented) and approved by the DAA.

(a) The DAAs of the participating ISs and the DAA of the overall network (if designated) will sign a Memorandum of Understanding (MOU).

(b) The DAA's approval will include a description of the classification and categories of information that can be sent over the respective networks.

(2) Connection between accredited ISs must be consistent with the sensitivity level and any other restrictions imposed by the accredited ISs. Unless the IS is accredited for multilevel operations and can reliably separate and label data, the IS is assumed to be transmitting the highest level of data present on the system during network connection.

(3) Employ identification, authentication, and encryption technologies when accessing network devices.

(4) Employ layered protective, filtering, and monitoring devices (for example, firewalls, IDSs) at enclave boundaries, managed access points, and key connection points.

(5) Periodically scan all installation assets and devices, implement protective measures, and report non-compliance as required (minimum is annually).

(6) Proxy all Internet access through a centrally managed access point and isolate from other DOD or Army ISs by physical or technical means.

f. E-mail security. E-mail systems will be used only for transmission and receipt of communications equivalent to or less than the classification level of the IS.

(1) IA personnel will—

(a) Promote security awareness.

(b) Use encryption when available or as part of the global enterprise (when implemented) to secure the sensitivity requirements of the data.

(c) Ensure the physical security of any information and the mail server.

(d) Install and configure antiviral software on e-mail servers and client workstations.

(e) Warn users to treat unusual e-mail messages the same way they treat unusual parcels—with caution.

(f) Use digital signatures to authenticate a message as needed (non-repudiation).

(g) Configure ISs to prevent opening attachments or active code directly from mail applications when available.

(2) Personnel will not share personal e-mail accounts. Commanders may allow the limited use of organizational or group e-mail accounts where operationally warranted.

(3) E-mail passwords will differ from the network password when used, until a global PKI initiative is available.

(4) Personnel will employ government owned or provided e-mail systems or devices for government communications and the use of commercial ISP or e-mail accounts for official purposes is prohibited.

(5) Auto-forwarding of official mail to non-official accounts or devices is prohibited.

(6) Permit communications to vendors or contractors to conduct official business and implement encryption and control measures appropriate for the sensitivity of the information transmitted.

(7) Personnel will scan all files for viruses before storing, transmitting, or processing information.

(8) Authorized users who are contractors, DOD direct or indirect hires, foreign nationals, or foreign representatives will have their respective affiliations displayed as part of their e-mail addresses.

g. Internet, Intranet, Extranet, and WWW security.

(1) Army Regulation 25–1 outlines requirements and policy on the use of Government-owned or leased computers for access to the Internet.

(2) Users are authorized to download programs, graphics, and textual information to a Government-owned IS as long as doing so does not violate federal and state law, regulations, acceptable use, and local policies (for example, configuration management, IA).

(3) Government-owned or leased ISs will not use commercial ISPs (for example, CompuServe, America on Line, Prodigy) as service providers, unless a government-acquired subscription to such services is in place and the access is for official business or meets the criteria for authorized personal use as indicated in AR 25–1, paragraph 6–1.

(4) Implement appropriate access, filtering, and security controls (for example, firewalls, restriction by IP address).

(5) Implement and enforce local area management access and security controls.

(6) Commercial ISP services are authorized to support those organizations identified in paragraph *b*(2), above and no cross connectivity to the NIPRNET will exist or be implemented.

(7) Prohibit public access to information not released for public disclosure.

(8) Extranet and intranet servers will provide adequate encryption and user authentication.

(9) Extranet servers and access will be approved through the installation IAM and DAA.

(10) All servers (including Web servers) that are connected to publicly accessible computer networks such as the Internet, or protected networks such as the SIPRNET, will employ a combination of access and security controls (for example, firewalls, routers, host-based IDSs) to ensure the integrity, confidentiality, accessibility, and availability of DOD ISs and data.

(11) Commanders and supervisors are responsible for complying with Federal, DOD, and DA Web site administration policies and implementing content-approval procedures that include OPSEC and PAO reviews before updating or posting information on all Web sites.

(12) Protect publicly accessible Army Web sites by placing them behind an Army reverse Web proxy server (as available). The reverse proxy server acts as a proxy for the intranet to the protected server, brokering service requests on behalf of the external user or server. This use of a reverse proxy server provides a layer of protection against Web page defacements by not allowing users to connect to the Web server directly.

(13) Publicly accessible Web sites not protected behind a reverse Web proxy (until moved) will be on a dedicated server in a DMZ, with all unnecessary services, processes, or protocols disabled or removed. Remove all sample or tutorial applications, or portions thereof, from the operational server. Supporting RCERTs and TNOSCs will conduct periodic vulnerability assessments on all public servers and may direct blocking of the site dependent on the inherent risk of identified vulnerabilities. Commanders or assigned IAMs will correct identified deficiencies.

(14) All private (non-public) Web sites that restrict access with password protection or specific address filtering are required to implement secure sockets layer (SSL) protocols utilizing a Class 3 DOD Public Key Infrastructure (PKI) certificate as a minimum. NETCOM issues and manages these certificates.

(15) Commander will conduct annual OPSEC reviews of all organizational Web sites and include these results in their annual OPSEC reports pursuant to AR 530–1.

(16) To verify compliance with Federal, DOD, and DA Web site administration policies, procedures, and best practices, the AWRAC will continuously review the content of publicly accessible U.S. Army Web sites to ensure compliance. (See also AR 25–1 for Web site administrative policies.) AWRAC will provide results from these assessments to commanders for corrective actions.

h. Approved keyboard, video, mouse (KVM) (keyboard, monitor, mouse (KMM)) switches. These devices are primarily introduced to achieve a reduction of hardware on the desktop and do not provide any IA features.

(1) These devices are not authorized for use for cross-domain interoperability (NIPRNET-to-SIPRNET or SIPRNET-to-NIPRNET guarding solution) network connections. See BBPs documentation on the CIO/G–6 IA Web site for approved items and implementation guidelines.

(2) Utilize screen-saver lockout mechanisms on all systems using a KVM/KMM switch.

i. Information Assurance tools. Use only IA security software listed on the IA Tools list on Army systems and networks. The list of Army approved IA tools is available through the ACERT or CSLA Web site. Requests for consideration and approval for additional security software packages to be added to the Army IA tools list must be submitted through NETCOM channels ATTN: NETC–EST–A, ATTN: IAD to CIO/G–6.

(1) Installation IAM-designated and Army-certified IA personnel may conduct tests under stringent conditions coordinated with the installation DOIM, IAM, TNOSC, and RCERT, at a minimum.

(2) RCIO IAPM approval, and advance notification of the servicing RCERT and TNOSC, is required before certified IA personnel may utilize public domain vulnerability assessment tools (for example, Nessus, Nmap, Saint, or Titan).

(3) Organizational IA personnel are prohibited from conducting penetration testing or attempts on ISs utilizing hacker tools or techniques. This restriction is applicable to operational networks and does not apply to those personnel or techniques used in a testing environment for C&A, vulnerability assessments of developmental systems, or used in a training environment for personnel certifications on isolated networks.

(4) Organizational IAMs can request penetration testing of their networks. Subordinate MACOM organizations may request penetration testing through their MACOM IAM to the installation IAM.

(5) The use of “keystroke monitoring” software of any kind is prohibited, except by LE/CI personnel acting within proper legal authority.

j. Networking security tools. The following policies apply to networking security tools used on Army ISs.

(1) Establish a security policy for each protection tool before purchase and implementation.

(2) Implement security tools within the security perimeter defensive architecture with NETCOM approval.

(3) Limit login access to internetworking devices to those individuals who operate and maintain those devices.

(4) Review configuration and audit files of security internetworking tools as a minimum on a weekly basis.

k. Other tools. Other tools employed by the Army include—

(1) Intrusion Detection Systems (IDSs). NETCOM, in coordination with CIO/G–6 and the ACERT, currently operates an IDS device for networks connected to the NIPRNET. Although NETCOM owns, operates, and maintains the enterprise IDS devices, this does not preclude the activity IA personnel from managing and analyzing local networks or the data. Local monitoring of an IDS is recommended with approval from the appropriate TNOSC. The request should document the operational requirement, the intent of monitoring, the software utilized, and the expected adverse effect if disapproved. Staff the request through the IAM to the RCIO IAPM and submit to the supporting RCERT/TNOSC. The requesting activity is responsible for providing the hardware and obtaining a copy of the NETCOM approved software. Coordinate the configuration of the software and reporting requirements with the supporting RCERT/TNOSC.

(2) Vulnerability scanners. Only individuals trained and certified will use assessment software. Before conducting mapping or scanning of a network, the IAM must notify the DOIM and the servicing RCERT/TNOSC with the purpose, start, and duration of the scanning activity.

(3) Copy of findings. Scan results will be provided to the servicing RCERT/TNOSC.

(4) Lack of expertise. Installations that do not have the expertise, requisite certification level, or resources to scan their own networks may request a vulnerability scan through their supporting RCERT/TNOSC.

(5) Unauthorized scans. Treat unauthorized scans of networks as potential intrusions and report upon detection. Persons conducting unauthorized scans of Army networks may be subject to administrative actions or punishment.

l. Tactical systems.

(1) Tactical systems, including weapon system and devices integral to weapon or weapon support systems, that include features normally associated with an IS will implement the requirements of this regulation and DODI 5200.40 (DITSCAP).

(2) When one or more of the minimum-security requirements are impractical or adversely impose risk of safety-of-use because of the function and design of the system, the situation will be addressed in the SSAA as well as in the C&A approval memorandum signed by the DAA.

(3) Mechanisms must be available to render the IS inoperable in case of imminent capture by hostile forces.

(4) Tactical networks connecting to standard tactical entry point (STEP) sites, garrison, or other fixed networks must be compliant with all security requirements (for example, configurations, approved software, C&A) before connection. They will be protected by access controls and intrusion detection systems in the same manner as garrison network defenses described earlier and will adopt a DiD strategy.

Section VIII
Incident and Intrusion Reporting

4–21. Information system incident and intrusion reporting

Incidents may result from accidental or deliberate actions on the part of a user or external influence. Evidence or suspicion of an incident, intrusion, or criminal activity will be treated with care, and the IS maintained without change, pending coordination with IA, ACERT/RCERT, and LE/CI personnel. Ensure users are aware of the policy governing unauthorized use of computer resources. Users will report all potential or malicious incidents because time-sensitive actions are required to limit the amount of damage or access. IS incidents will be reported within the command and to external agencies to assist LE or investigative agencies in compiling supporting evidence, impact assessments, associated costs, containment viability, and eradication and reconstruction measures necessary to effectively manage the breach and provide evidentiary material for prosecution.

a. Protect IS incident reports as a minimum FOUO or to the level for which the system is accredited.

b. Annually validate IS incident reporting procedures.

c. Report all IS incidents or events including, but not limited to—

(1) Known or suspected intrusion or access by an unauthorized individual.

(2) Authorized user attempting to circumvent security procedures or elevate access privileges.

(3) Unexplained modifications of files, software, or programs.

(4) Unexplained or erratic IS system responses.

(5) Presence of suspicious files, shortcuts, or programs.

(6) Malicious logic infection (for example, virus, worm, Trojan).

(7) Receipt of suspicious e-mail attachments, files, or links.

(8) Spillage incidents or violations of published BBP procedures.

d. A serious incident report (SIR) will be generated and reported per AR 190–40 under the following conditions—

(1) The incident poses grave danger to the Army's ability to conduct established information operations.

(2) Adverse effects on the Army's image such as Web page defacements.

(3) Access or compromise of classified or sensitive information (for example, soldier identification information (SSN), medical condition or status, patient-client or attorney-client privilege).

(4) Compromise originating from a foreign source.

(5) Compromise of systems that may risk safety, life, limb, or has the potential for catastrophic effects, or contain information for which the Army is attributable (for example, publicly accessible waterways navigational safety information from the USACE).

4–22. Reporting responsibilities

a. An individual who suspects or observes an unusual or obvious incident or occurrence will cease all activities and notify his or her SA/NA, IASO, or IAM immediately.

b. If the SA/NA, IASO, or IAM is not available, the individual will contact his or her supporting RCERT.

c. An SA/NA, IASO, or IAM who observes or suspects an incident or intrusion, or receives information on an incident, will logically isolate the system, prohibit any additional activities on or to the system, and immediately notify his or her supporting RCERT/TNOSC. Take no additional actions to investigate the incident until directed by the RCERT.

d. Isolation includes physical isolation (unplugging the network connection), restricting any direct physical access, and logical isolation (blocking the IP at security routers or firewalls both inbound and outbound) from the network to the system.

e. If the RCERT is not available then the SA or IASO will contact the ACERT directly. In addition, report per local supervisory reporting policies in effect.

f. Each RCERT is responsible for collecting and recording all the required information, coordinating all incident response procedures between LE/CI personnel and the organization, and conducting all intrusion containment, eradication, and verification measures.

g. The IS incident reporting format and additional reporting requirements are available on the ACERT and supporting RCERT NIPRNET/SIPRNET Web sites.

4–23. Compromised information systems guidance

a. When directed by RCERT, all ISs determined to be compromised either through unauthorized access or malicious logic will be rebuilt from original media, patched, and scanned for compliance before reintroduction to the network.

b. All similar ISs or devices on the affected network will be scanned for compliance or configuration management and SAs/NAs will immediately correct identified vulnerabilities. Report any additional ISs if suspected of compromise during this scanning phase.

c. Networks may require reaccreditations under the DITSCAP process following a successful compromise.

d. Specific details and actions for a compromised system are available on the ACERT Web site.

Section IX
Information Assurance Vulnerability Management

4–24. Information Assurance Vulnerability Management reporting process

a. General. The Information Assurance Vulnerability Management (IAVM) program supersedes the IAVA Program. IAVM compliance is the absolute minimum standard for all ISs, not the preferred end state, and is a proactive methodology of maintaining, patching, and updating systems before exploitation. IAVM requires the completion of four distinct phases to ensure compliance. These phases are: (1) vulnerability identification, dissemination, and acknowledgement; (2) application of measures to affected systems to make them compliant; (3) compliance reporting; and (4) compliance verification.

b. Responsibilities. The Army CIO/G–6 will be the POC to acknowledge receipt (within five days) of DOD CERT issued IAVM messages, aggregate compliance and waiver data, and report (within 30 days or as directed) to DOD. Systems and processes for collecting detailed information and for implementing IAVM are the responsibility of every IA person.

c. Army implementation of IAVM. ACERT will serve as the Army's focal point for initiation of the IAVM process.

(1) Vulnerability identification, dissemination, and acknowledgment. ACERT/ANOSC will issue Army IAVM messages. There are three types of DOD IAVM messages: alerts (IAVAs), bulletins (IAVBs), and TAs. DOD has restricted the use of these terms to the IAVM program only.

(a) IAVAs will establish mandatory suspense dates for acknowledgement and compliance, corrective actions to negate vulnerabilities, and implementation of additional CND requirements.

(b) IAVBs will establish mandatory suspense dates for acknowledgement yet allow commanders and IA personnel flexibility for implementation of the corrective actions to negate vulnerabilities or implementation of CND requirements. Corrective actions are required to be completed but not reported.

(c) Information Assurance technical tips (IATTs) (Army designation) allow commanders and IA personnel flexibility for acknowledgement and implementation to negate vulnerabilities or implement CND requirements. Acknowledgement and compliance is not reported. Corrective actions are required to be completed but not reported.

(d) All personnel responsible for implementing the IAVM process will register with the ACERT Listserve to receive messages. Use only official e-mail accounts for this distribution list.

(2) IAVM compliance. MACOM commanders, PEOs, PMs, and designated IA officers will disseminate implementation guidance as required and ensure implementation of IAVM requirements. Commanders or IA personnel will provide contractors, contracted support, or other personnel (as necessary) IAVM information as required to support compliance requirements.

4–25. Compliance reporting

a. NETCOM RCIOs, MACOM commanders, PEOs, PMs (or their IA officers), and garrison commanders will ensure that messages are acknowledged, corrective actions are implemented, extensions are requested, and compliance is reported to the compliance reporting database (CRD). Within 10 calendar days from the date of the IAVM, conduct a baseline assessment scan for affected assets and enter identified assets into the CRD. NETCOM RCIOs will oversee IAVM compliance reporting for their regions.

b. PEOs and PMs are responsible for implementing corrective actions for IAVM vulnerabilities that apply to systems under their proponency. Tactical systems will document compliance methodology in a classified addendum as part of the risk assessment or test report of the SSAA. The tactical system DAA-and only the tactical system DAA-will enforce or grant exemptions to IAVM compliance. DAAs will resolve compliance issues where it may result in safety or performance issues of a combat system that are operationally unacceptable.

c. If corrective actions required by issued alerts adversely affect operations, IAMs or their designated representatives (for example, affected SAs or IANMs) will conduct a risk assessment for the commander and contact their supporting RCIO, IAPM, or IAM. The RCIO, IAPM, or IAM will contact the Army CIO/G–6 through ACERT/NETCOM to request an extension, not to exceed 180 days, and to develop and implement an acceptable alternative security solution. The alternative security solutions must be coordinated with the ACERT/NETCOM before approval by the appropriate DAA. This extension request will include risk mitigation steps taken to reduce or eliminate the IAVM-identified risks until an acceptable solution is implemented.

d. Report IAVM compliance in the Army's CRD. To meet DOD requirements, register specific system/asset owners and SAs, including applicable electronic addresses, in the CRD.

e. All IAVM compliance reporting of classified, tactical, or operationally sensitive ISs will be through the CRD located on the SIPRNET.

4–26. Compliance verification

IAVA Compliance Verification Teams (CVTs) will conduct short-notice inspections of randomly selected units to verify compliance with IAVM messages.

a. Membership in the CVT may include a CIO/G–6 Team Chief; a vulnerability scan technician; U.S. Army Audit Agency representatives, operating under ARs 36–2 and 36–5; and U.S. Army Criminal Investigation Command representatives operating under AR 195–2.

b. In addition to reporting requirements under ARs 36–2, 36–5, and 195–2, the CVT will report to the inspected unit, the Army CIO/G–6, and the Senior Army Leadership. The Army CIO/G–6 will provide a copy to the appropriate MACOM, PEO, and PM CIOs.

c. Findings require a reply by endorsement on the corrective actions taken by the inspected command.

Section X
Miscellaneous Provisions

4–27. Vulnerability assessment programs

Several Vulnerability Assessment Programs and services are available throughout the Army. The ACERT/ANOSC provides comprehensive support in the areas of CND and IA Vulnerability Assessments; the U.S. Communications-Electronics Command (CECOM) provides assessments and support in the areas of platforms and IA architecture; the Army Research Laboratory (ARL) may provide support in the areas of survivability and lethality; and CID provides comprehensive crime prevention surveys. Only trained, authorized personnel will conduct vulnerability assessments of Army ISs.

a. Do-it Yourself Vulnerability Assessment Program (DITY VAP). Utilize the Do-it Yourself Vulnerability Assessment Program (DITY VAP) to assess configurations, compliance, asset identification, unauthorized connectivity, and security vulnerabilities within local network enclave borders. IAMs and IASOs will establish procedures to scan their networks quarterly to identify application, network, and operating system vulnerabilities, configuration errors, and points of unauthorized access.

(1) Scans will be properly coordinated within AOR between the initiating component and the supporting RCERT/TNOSC.

(2) Prohibit scans across network segments protected by a TNOSC security router or IDS, unless specifically coordinated and approved by NETCOM.

(3) DITY VAP assessments prohibit the use of data corruption, data manipulation, data denial, examination of data content, denial of service, or "hacking" and penetration tools and techniques.

(4) Train all IA participants on approved scanning tools and sign an acknowledgment of complete understanding of the "rules of engagement" before conducting any scanning activity. For example—

(a) No reading of personal data on networks while conducting a vulnerability assessment.

(b) No penetration testing.

(c) No denial-of-service attacks or tests.

(d) No scanning outside local network enclave borders.

b. Information Operations Vulnerability Assessments Division (IOVAD) Blue Team and Red Team Programs. The 1st IO CMD IOVAD offers assessment support in the areas of information management and security, in which focused efforts assess IA through the elements of OPSEC, COOP, INFOSEC, COMSEC, and CND. In addition, IOVAD Red Teams are available to challenge and assess readiness.

c. RCERT and TNOSC activities. RCERTs and TNOSCs may conduct no-notice remote scanning across enterprise boundaries, including, but not limited to, IAVM support, threat or asset identification, or vulnerable systems and services identification, with or without coordination with commanders or IA personnel. IA personnel will implement verification procedures to validate, but not hinder or deny, these scanning activities. RCERTs and TNOSCs may block or deny access to vulnerable systems identified during these scans until corrections have been made.

4–28. Portable electronic devices

Portable electronic devices (PEDs) are portable ISs or devices with the capability of wireless or LAN connectivity. These include, but are not limited to, cell phones, pagers, personal digital assistants (PDAs) (for example, Palm Pilots, Pocket PCs), laptops, and two-way radios. Current technologies (infrared, radio frequency, voice, video, microwave) allow the inclusion of several of these capabilities within a single device and dramatically increase the risks associated with IS and network access. Management of these devices will be as follows—

a. PEDs containing wireless communications or connectivity, audio, video, recording, or transmission capabilities will be prohibited from areas where classified information is discussed or electronically processed, unless specifically permitted as an exception by the DAA and all classification, access, and encryption restrictions are enforced for the PED as they would be for a classified device.

b. Implement identification and authentication measures at both the device and network level if connectivity is approved. Voice does not require DOD PKI IA.

c. PEDs will support PKI, digital certificates, FIPS, or NSA validated crypto modules or data encryption standards appropriate for the classification level of the information processed.

d. Provide all PED users with security awareness training regarding the physical and information security vulnerabilities and policies of the device.

e. Contractor provided or owned PEDs (if approved) will be stated as mission essential in contracts, and will meet all C&A standards and are subject to inspections and IA requirements as any other IS.

4–29. Wireless local area networks

Wireless LANs are extensions of wired networks and will implement IA policies and procedures in accordance with this and other applicable regulations. Non-compliant wireless LANs must have migration plans that ensure the systems will meet the minimum requirements of this policy. The DAA is responsible for maintaining these migration plans as part of his or her acceptable level of risk determination. All Army organizations and activities operating WLANs will comply with the following and as supplemented in BBPs——

a. Pilot and fielded wireless LANs and PEDs with LAN connectivity will meet the same C&A and IA security requirements as wired LAN ISs in accordance with this regulation, AR 380–53, AR 25–1, and DODIs 5200.40 and 8500.2.

b. DOIMs and IAMs must ensure that all WLANs that connect to the installation undergo NETCOM CCB and C&A processes.

c. Engineer wireless solutions to preclude backdoors.

d. Where wireless LANs are implemented or proposed, thorough analysis, testing, and risk assessments must be done to determine the risks associated with potential information intercepts or monitoring, TEMPEST emanations, and network vulnerability.

e. The use of AV software on wireless-capable ISs and devices is required.

f. Users will use access authentication on the system.

g. Control and monitor wireless access protocol (WAP) gateways, when approved, with firewalls and IDS devices.

h. Certify all wireless devices procured with Army funds for spectrum supportability through the Military Communications Electronics Board (MCEB) per DODD 5000.1 and AR 5–12. Submit spectrum supportability requests to NETCOM/9th ASC, ATTN: NETC–EST–V, Suite 1204, 2461 Eisenhower Ave, Alexandria, VA 22331–0200.

i. Terminate wireless access points at a boundary device in the DMZ, not in the internal enclave.

j. Certify that WLAN frequencies meet any host nation or government restrictions.

4–30. Employee-owned information systems

a. Prohibit the use of employee-owned information systems (EOISs) for classified or sensitive information.

b. The use of an EOIS for ad-hoc (one-time or infrequent) processing of unclassified information is restricted and only permitted with IAM, DAA, or commander approval. Requirements for use and approval are included in AR 25–1, paragraph 6–1e.

c. If approved for ad hoc use, EOISs processing official data will comply with all security provisions of this regulation. Computer owners will implement IA countermeasures required by this regulation, specifically AV and IA software and updates, or be prohibited from such activity. All processed data will be removed from the EOIS and personnel will sign compliance statements that the data was removed.

d. Include security requirements and authorized software availability for the use and safeguarding of EOISs in security training.

e. Contractor-owned and operated ISs will meet all security requirements for government-owned hardware and software when operating on the AEI or conducting official business.

f. Scan all data processed from an EOIS before inclusion or introduction into the network.

g. Prohibit all remote access for remote management from EOISs.

4–31. Miscellaneous processing equipment

There is a variety of non-COMSEC-approved miscellaneous process equipment (MRE) involved with classified information. This includes copiers, facsimile machines, peripherals, electronic typewriters, word processing systems, and others. Activities must identify those features, parts, or functions used to process information that may retain all or part of the information. Security procedures must prescribe the appropriate safeguards, in accordance with chapter 7, AR 380–5 to prevent unauthorized accesses to either the information or equipment.

a. Digital copiers, printers, scanners, faxes, and similar IS devices employ embedded hard-drives or other media that may retain residual classified or sensitive information. Include these devices as part of the C&A process.

b. Destroy replaced equipment parts per classification level when removed.

c. Cleared and technically qualified personnel will inspect equipment before equipment removal from protected areas.

d. Peripheral devices (for example, printers, copiers) are subject to IAVM compliance and accreditation.

e. Peripheral devices (for example, printers, copiers) are subject to sanitizing, purging, or disposition restrictions as published.

Chapter 5
Certification and Accreditation

5–1. Certification and accreditation overview

a. This chapter outlines the policies governing the security C&A of Army ISs and networks in accordance with DOD Directive 8500.1, DOD Instruction 8500.2, P.L. 100–235 (Computer Security Act of 1987), OMB Circular A–130, DOD Directive 5220.22, DOD 5220.22M, and DOD 5220.22–M–SUP. Basic goals of the C&A process include ensuring that C&A efforts will be appropriate to the system being evaluated as well as cost effective.

b. All Army ISs will be certified and accredited in accordance with DODI 5200.40 (DITSCAP). Perform certification and accreditation of Army ISs according to the type accreditation process or by the site-based accreditation process. In addition, the IS being accredited may be considered as a single system or LAN. DODIIS systems will be accredited in accordance with DCID 6/3, Annex (JDCSISSS), DIAM 50–4, and other applicable instructions and regulations.

c. Include a threat analyst (that is, NETCOM G–2) as part of the DITSCAP process.

d. Consider vendor integrity statements (VISs) when available from DISA, which verify that vendor software will not affect the integrity of operating systems when utilized.

e. Consider foreign-ownership, influence, or interests during threat evaluations of software development or IS C&A packages.

f. Incorporate published or established NETCOM CCB and networthiness certification requirements during the C&A process.

5–2. Certification

a. Security certification is a comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards made in support of the accreditation process. It establishes the extent to which a particular design and implementation meets a set of specific security requirements.

b. The certifier will coordinate with technical personnel to conduct a certification test under a certification plan to determine if an unclassified, sensitive, or classified system adequately meets prescribed security policy objectives.

c. Certifiers will include a CSLA cryptographic advisor on the certification team throughout the C&A effort until the DAA signs the SSAA to ensure current and future compliance of crypto requirements.

d. Certification primarily addresses software, hardware, firmware, and data security measures. It must also consider procedural, physical, personnel, threat, and emissions security to enforce security policy.

5–3. Tailoring

a. The time and labor expended in the C&A process must be proportional to the system size, criticality, and mode of operation, data sensitivity, and number of users.

b. The activities defined in the four phases of the DITSCAP are mandatory. However, tailor implementation details of these activities and, where applicable, integrate with other acquisition activities and documentation.

5–4. Accreditation

a. Accreditation is the official management authorization to operate an IS or network and is based, in part, on the formal certification of the degree to which a system meets a prescribed set of security requirements. The C&A statement affixes security responsibility with the accrediting authority.

b. Accreditation must address each operational environment of the IS for both fixed and deployable configurations. For example, an IS may operate at one sensitivity level in a standalone mode and connect to a global network with another sensitivity level. The C&A must clearly establish procedures for transition between the two environments. Multiple operational environments can result in multiple accreditations for a single IS if different DAAs are involved. However, in the concept of the operations document, a single accreditation that addresses all variations is sufficient. Refer to CIO/G–6 IA Directorate Web site BBPs for further guidance and procedures on IS accreditation.

c. Site-based accreditations can be for a single unit or for a LAN with appropriately accredited ISs generally performing similar functions with similar equipment.

d. Type accreditations must indicate whether they are generic or operational accreditations and are certifications for ISs or applications fielded by program managers to different locations, and must be defined as a single or group of systems.

5–5. Re-accreditation

a. Re-accredit ISs under this regulation within a period of 3 years from its latest C&A. If none of the events listed in paragraph b, below has occurred, this re-accreditation may consist of a simple review and update of the accreditation documentation.

b. A new or updated accreditation is required beginning with Phase 1 of the DITSCAP if any of the following events occurs—

(1) Addition or replacement of a major component or a significant part of a major system.

(2) A change in classification level of information processed.

(3) A change in security mode of operation.

(4) A change in interfacing systems.

(5) A significant change to the operating system or executive software.

(6) A breach of security, violation of system integrity, or any unusual situation that appears to invalidate the accreditation.

(7) A significant change to the physical structure housing the IS or environment of the IS that could affect the physical security described in the accreditation.

(8) A significant change to the threat that could adversely affect Army systems.

(9) A significant change to the availability of safeguards.

(10) A significant change to the user population.

5–6. Accreditation documentation

a. The ATO or the interim approval to operate (IATO) and complete C&A documentation will be forwarded to the senior IA person of each Army MACOM and each major installation or activity IAM receiving the system following functional DAA and NETCOM RCIO approval. The MACOM IAPM, together with the command functional user representative and NETCOM RCIO, will review the C&A documentation and either accept the ATO or IATO or prescribe additional measures or procedures to meet the needs of a unique operating environment. Such additional measures will be appended to the system accreditation. Upon acceptance, the RCIO or MACOM IAPM will publish a memorandum authorizing system use in that MACOM.

b. Approval to operate is contingent on the following conditions—

(1) Issue an ATO if the system meets the requirements stated in the Systems Security Authorization Agreement (SSAA) per paragraph 5–4 of this regulation and DODI 5200.40 (DITSCAP).

(2) An ATO is valid for a maximum period of 3 years, and must be renewed in accordance with paragraph 5–5 of this regulation.

c. IATO is contingent on the following conditions—

(1) Issue an IATO if the system does not meet the requirements stated in the SSAA, but mission criticality mandates that the system become operational.

(2) Change an IATO to an ATO when the SSAA requirements are validated.

(3) IATOs are valid for 180 days; review them monthly until the ATO is granted.

(4) A maximum of two IATOs will be granted.

(5) Provide an IATO risk management protection plan to the IAPM and MACOM to mitigate associated risks during the IATO.

5–7. Connection approval process

a. Army organizations requiring network access to the Defense Information Systems Network (DISN) will prepare a CAP package requesting connection approval. The DAA of the DISN node will provide guidance to organizations connecting to them for access to the DISN. The DAA will approve the connection request and issue an approval to connect.

b. Interconnection of two or more enclaves requires DAA approval through MOUs or Memoranda of Agreement (MOAs) between all DAAs. MOUs/MOAs will address interconnection requirements as outlined in DODI 8500.2.

5–8. Designated approving authorities

a. A DAA will be appointed for every IS and network.

b. CIO/G–6 will maintain a list of DAAs for all systems fielded by a DA staff element or by a DA-chartered PM.

c. A DAA will be appointed for every IS and network as follows—

(1) For site-based accreditation, the following conditions apply—

(a) The following individuals are accreditation officials for SCI and SIOP–ESI systems——

1. The Director, Defense Intelligence Agency is the DAA for those systems processing SCI with connection to the Joint Worldwide Intelligence Communications System (JWICS).

2. The DCS, G–2 is the C&A authority for SCI systems operating at Protection Level 1 or 2 in accordance with DCID 6/3.

3. The Director, National Security Agency is the DAA for cryptographic solutions.

4. The Director, Joint Staff is the DAA for systems that process SIOP–ESI data.

(b) NETCOM commander and the Administrative Assistant to the Secretary of the Army (acting as the HQDA POC) are the accreditation authorities and may further delegate, in writing, accreditation authority. Such delegation may be by name or by established position titles.

1. For TS collateral systems, delegate to general officers, a MACOM senior intelligence officer (SIO), or to Senior Executive Service personnel within their commands or agencies.

2. For SECRET ISs, delegate to personnel at the minimum rank/grade of colonel or GM/GS/GG–15 who are occupying a position of command or a principal staff office at an installation or general officer command.

3. For sensitive ISs, to personnel who are in the minimum rank/grade of lieutenant colonel or GM/GS/GG–14.

(2) For Type accreditation, the following conditions apply—

(a) The Director, DIA is the DAA for systems processing SCI that meet the following criteria—

1. Operate or are planned to operate in the compartmented or multilevel security mode or that require connection to an external network.

2. Have received special approval from DIA for a generic accreditation. This approval applies only to systems fielded in identical configurations at a large number of sites. The DIA may require additional measures such as configuration control.

(b) The DCS, G–2 is the DAA for SCI systems not covered above (Protection Levels 1 and 2 in DCID 6/3).

(c) The CIO/G–6 is the DAA for TS and below ISs in the multilevel security mode.

(d) The applicable PEO, with concurrence from CIO/G–6, is the DAA for systems not described above. When a Type accreditation is appropriate and the IS is not being fielded through the PEO structure, a general officer or a member of the Senior Executive Service who has responsibility for fielding the system may be appointed as the DAA with concurrence from CIO/G–6.

(e) If a Type accreditation is appropriate and the DAA is not readily apparent from the above guidance, contact CIO/G–6 for assistance to determine the DAA.

d. Accreditation of signals intelligence (SIGINT) systems is the responsibility of the Director, NSA.

e. Temporary sub-delegation of DAA authority may be granted if an operational or organizational requirement occurs that prevents the DAA from performing his or her primary responsibilities (for example, deployment, temporarily reassignment, hospitalization). This sub-delegation is valid for issuance of an IATO only for that organization's SECRET and below ISs.

Chapter 6
Communications Security

6–1. Communications security overview

This chapter provides DA policy for the acquisition, implementation, and life-cycle management of cryptographic systems, products, and services used to protect sensitive and classified national security information, systems, and networks.

a. Protection of classified national security information and systems. Only NSA-approved cryptographic systems will be used to protect classified national security information and national security systems.

(1) Classified national security information will be protected in transmission by NSA Type 1 cryptography.

(2) For the purposes of this regulation, all tactical information systems are considered as being critical to the direct fulfillment of military or intelligence missions, and therefore are regarded as national security systems. Tactical information systems will be protected by NSA-approved Type 1 cryptography. Only in exceptional circumstances, approved on a case-by-case basis by CIO/G–6, will NIST/NIAP-approved cryptographic systems (see para 6–1b, below) or foreign cryptographic systems (see para 6–1c, below) be employed in the tactical force structure.

(3) Requirements for NSA-approved cryptographic systems will be identified and validated in the AIAP and managed by the Army Information Assurance Directorate.

(4) NSA cryptographic systems will be centrally acquired and managed by the CSLA.

(5) Only keying material produced by NSA or generated by NSA-approved key generators will be used to key cryptographic systems that protect classified national security information.

(6) All cryptographic systems employed in the tactical force structure must be capable of being supported by the Army EKMS/KMI. Systems not capable of being supported by Army EKMS will be identified as non-compliant and phased out of service as soon as possible. Each approved cryptographic system will have a key management plan that describes in detail all activities involved in the handling of cryptographic keying material for the system, including other related security parameters (such as IDs and passwords). The plan will describe accountability over the keying material over the entire life cycle of the system's keys from generation, storage, distribution, and entry into the system through use, deletion, and final destruction.

b. Protection of unclassified and sensitive information and systems. Cryptographic systems or products intended for the protection of unclassified sensitive information and systems will—

(1) Employ cryptographic modules that have been validated under the NIST Cryptographic Module Validation Program (CMVP) as meeting, at a minimum, level 2 security requirements of the Federal Information Processing Standard 140–2 (FIPS 140–2).

(2) Be evaluated by a NIAP-certified common criteria testing laboratory, and at a minimum, meet all requirements of evaluation assurance level 3 and the common criteria controlled access protection profile.

(3) Products that meet higher FIPS 140–2 security requirements and common criteria evaluation assurance levels will be given preference.

(4) Requirements for NIST/NIAP-approved cryptographic systems intended to protect unclassified sensitive information will be identified and validated in the AIAP, managed by the Army Information Assurance Directorate (IAD). Funding for these systems will be the responsibility of the organization or activity identifying the requirement.

(5) All NIST/NIAP-approved cryptographic systems will be centrally acquired and managed through CSLA.

(a) There are three FIPS symmetric key algorithms approved for the protection of unclassified and sensitive information. They are: the Advanced Encryption Standard (AES), Triple-Data Encryption Standard (Triple-DES), and Skipjack. AES is the FIPS-approved symmetric encryption algorithm of choice.

(b) The Data Encryption Standard (FIPS 46–2) was superseded by Triple-DES (FIPS 46–3) on March 25, 2000. Within the Army, implementations of DES will be completely phased out of operation by 30 June 2004.

(c) All Army implementations of Triple-DES will use three different 56-bit keys.

(6) Each NIST/NIAP-approved cryptographic system will have a key management plan that describes in detail all activities involved in the handling of cryptographic keying material for the system, including other related security parameters (such as IDs and passwords). The plan will describe accountability over the keying material over the entire life cycle of the system's keys from generation, storage, distribution, and entry into the system through use, deletion, and final destruction.

(7) Only keying material produced by NSA, or generated by NSA-approved key generators, will be used to key cryptographic systems protecting unclassified sensitive information and systems. Vendor-unique or proprietary key management systems that require continued reliance by the Army upon a vendor to produce keying material will be phased out by 31 December 2005. Exceptions to this requirement will be approved by the Army IAD. Developmental systems will begin migration toward network-over-the air (NOTA) rekey.

(8) All HQDA authorized (see para 6–1a(2), above) NIST/NIAP-approved cryptographic systems employed in the tactical force structure must be capable of being supported by the Army EKMS. Systems presently in use that are not capable of being supported by Army EKMS will be phased out of service by 31 December 2005.

c. Use of NIST or foreign cryptographic systems to protect national security information and systems. With the exception of those systems approved by NSA and endorsed by HQDA, at no time will U.S. classified national security information be protected by foreign cryptographic systems or products, or by a NIST/NIAP common criteria testing laboratory evaluated product.

(1) Exceptions will be re-approved on an annual basis.

(2) Use of any unapproved product to protect classified national security information will be considered as a reportable communications security incident under paragraph 7–3b of AR 380–40, and punitive measures will be taken.

d. Advanced Encryption Standard. Federal Information Processing Standard Number 197 (FIPS 197), dated 26 November 2001, promulgated and endorsed the Advanced Encryption Standard as the approved algorithm for protecting sensitive (unclassified) information. NSA has conducted a review and analysis of AES and its applicability to protect classified national security information and systems. The design and strength of all key lengths of the AES algorithm (that is, 128, 192, and 256) are sufficient to protect classified national security information up to the SECRET level. TOP SECRET information will require the use of either the 192 or 256 key length. Achieving a desired level of protection is dependent on more than just key length; the implementation of the algorithm is equally important. The implementation of AES in products intended to protect classified national security information and systems must be reviewed and certified by NSA, and approved by CIO/G–6 prior to their acquisition through CSLA.

e. Public key cryptography. Systems that employ public key (asymmetric key) technology to protect unclassified sensitive or classified national security information and systems will be approved by the CIO/G–6. Asymmetric keys will be obtained through authorized DOD or Army certificate authorities operating under current DOD-approved Certificate Practice Statements.

f. Approved Cryptographic Systems and Algorithms. CSLA will maintain a list of approved cryptographic systems and algorithms for use in the Army. All cryptographic products must be procured through CSLA to be valid for use on an Army system.

6–2. Protected distribution systems

a. A protected distribution system (PDS) will be used only if cost-effective and sufficiently controlled to prevent covert penetration and interception.

b. Any IS that includes a PDS to transmit data will not be operationally accredited until the PDS has been approved.

c. PDSs must be constructed per criteria contained in NSTISSI No 7003 and supplemented with IA procedures in this regulation.

6–3. Approval of protected distribution systems

a. Authority to approve a PDS for the clear text transmission of classified information within fixed plant and garrison installations is delegated as follows—

(1) Principal HQDA officials for activities under their staff supervision, direction, or control.

(2) Garrison commanders for their organic activities.

b. Requests for approval of a PDS to transmit TS information must include an evaluation by the appropriate support element. Approval authorities may request technical assistance from INSCOM, 902nd MI Group, Fort Meade, MD 20755, in applying security criteria and processing the approval action for other PDSs.

c. Commanders of battalion and higher echelons may approve circuits for clear text electrical transmission of SECRET and CONFIDENTIAL information in tactical environments. Under combat conditions, commanders may delegate this authority to the company level. Tactical PDSs will not be approved for clear text transmission of TS information.

d. Once a PDS has been approved, no changes in installation, additions, or use may be made until the approval authority has granted approval for such changes.

e. Requests to approve a PDS will be submitted through channels to the installation IAM and DAA. Requests will be classified at least CONFIDENTIAL and will contain the following information—

(1) Full identification and location of the requesting organization.

(2) A statement of the classification of information to be transmitted on the PDS.

(3) A copy of the building floor plan (or a diagram of the field area as appropriate) designating the following—

(a) Proposed cable route and location of subscriber sets, distribution frames, junction boxes, and any other components associated with the circuit.

(b) Other wiring along the PDS route.

(4) Description of the cable installation (for example, 24 pairs of shielded cable in rigid steel conduit, 6 pairs of shielded cable in floor, or fiber optic cable). Indicate the cable length.

(5) Description and nomenclature of terminal and subscriber equipment to be used.

(6) Clearance of individuals having access to the circuit.

(7) Type of guards (for example, U.S. military, U.S. civilian, foreign civilian) and their security clearance or access authorization status.

(8) Description of access control and surveillance of uncleared personnel who may be allowed entry into the area housing any part of the PDS.

(9) Identification of the power source to be used for the PDS and a statement of the distance to the nearest point where undetected tampering would be possible.

(10) A justification for using the proposed PDS.

(11) A statement concerning any deviations from the established PDS criteria and an evaluation of their security implications.

(12) For PDSs to be used with TS information, a copy of the security evaluation.

6–4. Radio systems

a. Protect all voice or data military radio systems and COTS-implemented cellular or wireless communications devices and services to the level of sensitivity of the information.

b. Use electronic, auto-manual, or manual crypto-systems to provide the needed security for existing radio systems that do not have embedded or electronic crypto-systems. However, all future procurements must comply with paragraph 6–1, above.

c. Prohibit the use of commercial non-encrypted radio systems in support of command and control functions.

d. Radios used for public safety communications with civil agencies or to communicate on civil aviation channels are excluded from the requirements of paragraphs a and b, above. This exclusion does not apply to communications dealing with aviation combat operations.

6–5. Telecommunication devices

a. Government-owned equipment; receiving, transmitting, recording, and amplification equipment; or other non-secure telecommunications equipment will not be used unless declared in writing by the local commander as mission essential before use in such restricted areas as classified work areas, mission essential vulnerable areas (MEVAs), or staging areas before deployment. The DAA remains the accreditation authority for telecommunication devices in restricted areas. Failure to comply with this policy relating to the unauthorized use of telecommunication devices in restricted areas may subject the offender to administrative action, punishment, or other authorized adverse action.

b. Use only NSA-approved secure telephone units to discuss classified information.

c. Privately owned receiving, transmitting, recording, amplification, and processing equipment is prohibited from use within the confines of any area designated or excluded by the commander to be a classified work area, restricted area, mission essential vulnerable area, or staging area before deployment.

Chapter 7
Risk Management

7–1. Risk management process

a. Absolute confidence in the information accessed or available in the Army enterprise is unachievable; as such, the Army and DOD will approach increasing that level of trust through the implementation of a risk management process. With technological advances and capabilities, training, and IA-focused processes to reduce identifiable threats, the level of trust of information and ISs is significantly increased. Establish a risk management process containing the following phases as a minimum for all Army ISs. The process outlined in this chapter is based, in principle, on the risk management doctrine as defined by FM 100–14—

(1) Identify threats such as those posed by default designs or configurations, architecture deficiencies, insider access, and foreign or nation-state interests and capabilities.

(2) Assess threats to determine risks. What information is accessible? Who has authorization to access the information? What is the potential adverse effect of loss, access, or manipulation of the data? What are the OPSEC issues of data availability? What are the data owner's requirements?

(3) Develop controls and make risk management decisions. How do you protect the information, access, and infrastructure?

(4) Implement controls, countermeasures, or solutions and monitor for compliance and success.

(5) Supervise, evaluate, review, and refine as necessary.

b. Commanders, combat developers, and materiel developers will integrate the risk management process in the planning, coordination, and development of Army ISs.

c. Reevaluate and reissue any risk analyses and mitigations plans if there is a successful compromise of an IS or device.

d. Telecommunications systems that do not include the features normally associated with an IS and that handle classified or sensitive information will be implemented and operated in conformance with the risk management process.

7–2. Information operations condition

The IAPM or senior MACOM IA person is responsible for coordinating an INFOCON plan. The INFOCON is a

Commander’s Alert System that establishes a uniform DOD and Army process for posturing and defending against malicious activity targeted against DOD ISs and networks. The countermeasures at each level will be available under a BBP when published or as directed by the combatant command when the MACOM is a Service component command. If there is a conflict between Army and combatant command directed measures, those of the combatant command take precedence. Typical countermeasures include preventative actions and actions taken during an attack as well as damage control and mitigation actions. Measures will be addressed as a BBP when developed.

Appendix A
References

Section I
Required Publications

AR 25–1
Army Information Management. (Cited in paras 3–3j, 3–3l, 4–20c, 4–20g, 4–29a, 4–30b.)

AR 380–5
Department of the Army Information Security Program. (Cited in paras 3–3c, 4–11a, 4–11d, 4–16a, 4–17c, 4–31.)

AR 380–53
Information Systems Security Monitoring. (Cited in paras 3–2e, 4–5m, 4–5s, 4–29a.)

DA PAM 25–1–1
Installation Information Services. (Cited in para 4–5h.)

Section II
Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AR 5–12
Army Management of the Electromagnetic Spectrum

AR 25–55
The Department of the Army Freedom of Information Act Program

AR 36–2
Audit Reports and Followup

AR 36–5
Auditing Service in the Department of the Army

AR 70–1
Army Acquisition Policy

AR 190–40
Serious Incident Report

AR 195–2
Criminal Investigation Activities

AR 340–21
The Army Privacy Program

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380–15
Safeguarding Classified NATO Information

AR 380–19
Information Systems Security

AR 380–40
Policy for Safeguarding and Controlling Communications Security (COMSEC) Material

AR 380–49
Industrial Security Program

AR 381–10
U.S. Army Intelligence Activities

AR 381–11
Production Requirements and Threat Intelligence Support to the U.S. Army

AR 381–14
Technical Surveillance Countermeasures (TSCM)

AR 381–20
The Army Counterintelligence Program

AR 525–13
Antiterrorism

AR 530–1
Operations Security (OPSEC)

Chairman of the Joint Chiefs of Staff Instruction 5221.01
Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations. (http://www.dtic.mil/cjcs_directives/)

Chairman of the Joint Chiefs of Staff Manual 6510.01
Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND) (http://www.dtic.mil/cjcs_directives/)

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model; Part 2: Security functional requirements; Part 3: Security assurance requirements (http://niap.nist.gov/)

DOD Directive 5000.1
The Defense Acquisition System. (http://www.dtic.mil/whs/directives)

DOD 5000.2–R
Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs (http://dod5000.dau.mil/)

DOD 5200.2–R
Personnel Security Program (http://www.dtic.mil/whs/directives)

DOD 5220.22–M
National Industrial Security Program Operating Manual (http://www.dtic.mil/whs/directives)

DOD 5220.22–M–SUP
National Industrial Security Program Operating Manual Supplement (http://www.dtic.mil/whs/directives)

DOD Directive 5220.6
Defense Industrial Personnel Security Clearance Review Program (http://www.dtic.mil/whs/directives)

DOD Directive 5220.22
DOD Industrial Security Program (http://www.dtic.mil/whs/directives)

DOD 5400.7–R
DOD Freedom of Information Act Program (http://www.dtic.mil/whs/directives)

DOD 5500.7–R
Joint Ethics Regulation, Acceptable Use Policies, and the Standards of Ethical Conduct (http://www.dtic.mil/whs/directives)

DOD 8510.1–M
Department of Defense Information Technology Security and Accreditation Process Application Manual (http://www.dtic.mil/whs/directives)

DOD Directive 5230.9
Clearance of DOD Information for Public Release (http://www.dtic.mil/whs/directives)

DOD Directive 5230.11
Disclosure of Classified Military Information to Foreign Governments and International Organizations (http://www.dtic.mil/whs/directives)

DOD Directive 5230.25
Withholding of Unclassified Technical Data From Public Disclosure (http://www.dtic.mil/whs/directives)

DOD Directive 8500.1
Information Assurance (http://www.dtic.mil/whs/directives)

DOD Instruction 5200.40
DOD Information Technology Security Certification and Accreditation Program (DITSCAP) (http://www.dtic.mil/whs/directives)

DOD Instruction 8500.2
Information Assurance (IA) Implementation (http://iase.disa.mil/policy.html)

Defense Intelligence Agency Manual 50–4
Security of Compartmented Computer Operations. (Information may be obtained from the Defense Intelligence Agency, 200 MacDill Blvd, Bldg 6000, Bolling AFB, Washington, DC 20340.)

Director, Central Intelligence Agency Directive 1/7
Security Controls on the Dissemination of Intelligence Information (http://www.cms.cia.sgov.gov/dci/policy/dcid/default.htm)

Director, Central Intelligence Agency Directive 5/6
Intelligence Disclosure Policy (http://www.cms.cia.sgov.gov/dci/policy/dcid/default.htm)

Director, Central Intelligence Agency Directive 6/3
Protecting Sensitive Compartmented Information within Information Systems (http://www.cms.cia.sgov.gov/dci/policy/dcid/default.htm)

Field Manual 100–6
Information Operations

Field Manual 100–14
Risk Management

Federal Information Processing Standards Publication 140–2
Security Requirements for Cryptographic Modules (http://www.itl.nist.gov/)

Joint DODIIS
Cryptologic SCI Information Systems Security Standards (http://www.nmic.navy.smil.mil/onihome-s/security/sso_navy/policyNpubs/jdcsisss/jdcissi-r2.html)

JTA–A
Joint Technical Architecture-Army (https://www.us.army.mil) (all documentation is available on AKO site in collaborative center that you must subscribe to)

HQDA LTR 25–02–1
U.S. Army Wireless Local Area Networks

HQDA LTR 25–03–1
Transition of Information Duties and Responsibilities

NSTISSI No. 4012
National Training Standard for Designated Approving Authority (DAA) (http://www.nstissc.gov)

NSTISSI No. 4015
National Training Standard for System Certifiers (http://www.nstissc.gov)

NSTISSI No. 7003
Protective Distribution Systems (http://www.nstissc.gov)

NSTISSP No. 11
National Information Assurance Acquisition Policy (http://www.nstissc.gov)

Office of Management and Budget Circular A–130
Management of Federal Information Resources (http://www.whitehouse.gov/)

Public Law 100–235
Computer Security Act of 1987 (http://www.gpoaccess.gov/nara/)

Public Law 107–314
Bob Stump National Defense Authorization Act for Fiscal Year 2003 (http://www.gpoaccess.gov/nara/)

UCMJ
Uniform Code of Military Justice

5 USC 552a
The Privacy Act of 1974 (http://www.gpoaccess.gov/uscode/index.html)

22 USC 2751
Arms Export Control Act (http://www.gpoaccess.gov/uscode/index.html)

RCS CSIM–62
MDEP M54X Report

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

These forms are available on the APD Web site (www.apd.army.mil) and the Army Electronic Library (AEL) CD–ROM.

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 254
DOD Contract Security Classification Specifications

SF 328
Certificate Pertaining to Foreign Interests (available on GSA Web site@http://www.GSA.GOV/Forms)

Appendix B
Sample Acceptable Use Policy

B–1. Purpose

This appendix provides a sample Acceptable Use Policy (AUP) that may be used by organizations to obtain explicit acknowledgements from individuals on their responsibilities and limitations in using Army ISs.

B–2. Explanation of conventions in sample Acceptable Use Policy

Figure B–1 below illustrates a representative AUP. In this figure, text appearing in italicized font should be replaced with the appropriate information pertinent to the specific AUP being executed. Army organizations may tailor the information in the sample AUP to meet their specific needs, as appropriate.

Acceptable Use Policy

1. Understanding. I understand that I have the primary responsibility to safeguard the information contained in *classified network name (CNN)* and/or (*unclassified network name (UNN)* from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

2. Access. Access to *this/these* network(s) is for official use and authorized purposes and as set forth in DOD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.

3. Revocability. Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. Classified information processing. *CNN* is the primary classified Information System (IS) for (*insert your organization). CNN* is a *US-only system* and approved to process (*insert* classification) collateral information as well as: (*insert additional caveats or handling instructions*). *CNN* is not authorized to process (*insert classification or additional caveats or special handling instructions).*

a. *CNN* provides communication to *external DOD (or specify other appropriate U.S. Government)* organizations using the *SIPRNET.* Primarily this is done via electronic mail and internet networking protocols such as *web, ftp, telenet (insert others as appropriate).*

b. The *CNN* is authorized for *SECRET* or lower-level processing in accordance with *accreditation package number, identification, etc.*

c. The classification boundary between *CNN* and *UNN* requires vigilance and attention by all users. *CNN* is also *a US-only system* and not accredited for transmission of *NATO* material.

d. The ultimate responsibility for ensuring the protection of information lies with the user. The release of *TOP SECRET* information through the *CNN* is a security violation and will be investigated and handled as a security violation or as a criminal offense.

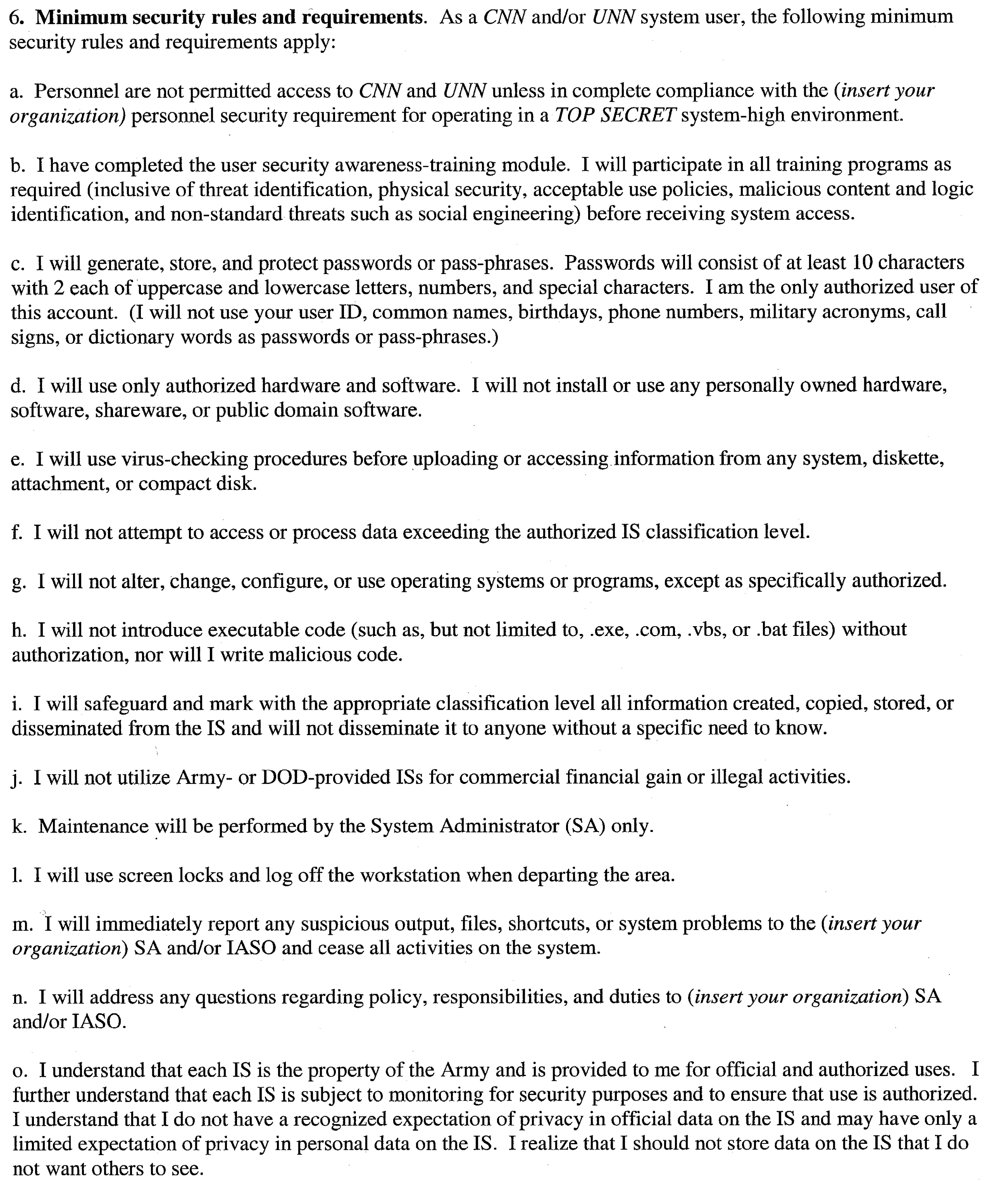
5. Unclassified information processing. *UNN* is the primary unclassified information system for the (i*nsert your organization). UNN* is a *US-only system.*

a. *UNN* provides unclassified communication to external DOD and other United States Government organizations. Primarily this is done via electronic mail and Internet networking protocols such as *web, ftp, telnet (insert others as appropriate).*

b. *UNN* is approved to process *UNCLASSIFIED, SENSITIVE* information in accordance with *(insert local regulation dealing with automated information system security management program).*

c. The *UNN* and the Internet, as viewed by the (*insert your organization),* are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet.

Figure B–1A. Acceptable Use Policy



6. **Minimum security rules and requirements**. As a *CNN* and/or *UNN* system user, the following minimum security rules and requirements apply:

a. Personnel are not permitted access to *CNN* and *UNN* unless in complete compliance with the (*insert your organization)* personnel security requirement for operating in a *TOP SECRET* system-high environment.

b. I have completed the user security awareness-training module. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.

c. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. (I will not use your user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords or pass-phrases.)

d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.

e. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk.

f. I will not attempt to access or process data exceeding the authorized IS classification level.

g. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

i. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

j. I will not utilize Army- or DOD-provided ISs for commercial financial gain or illegal activities.

k. Maintenance will be performed by the System Administrator (SA) only.

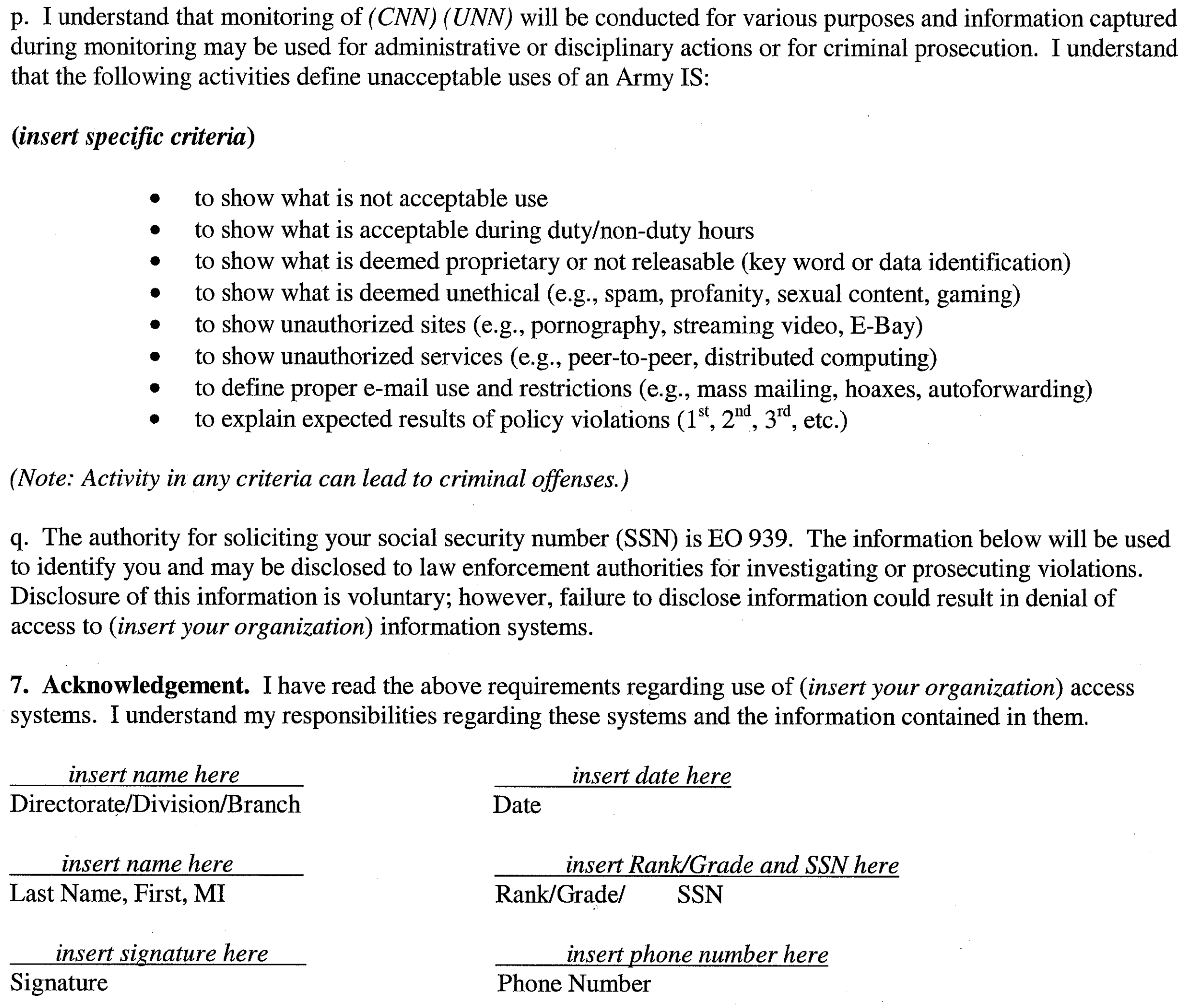
l. I will use screen locks and log off the workstation when departing the area.

m. I will immediately report any suspicious output, files, shortcuts, or system problems to the (*insert your organization*) SA and/or IASO and cease all activities on the system.

n. I will address any questions regarding policy, responsibilities, and duties to (*insert your organization*) SA and/or IASO.

o. I understand that each IS is the property of the Army and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

Figure B–1B. Acceptable Use Policy-Continued



p. I understand that monitoring of *(CNN) (UNN)* will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities define unacceptable uses of an Army IS:

(insert specific criteria)

- to show what is not acceptable use
- to show what is acceptable during duty/non-duty hours
- to show what is deemed proprietary or not releasable (key word or data identification)
- to show what is deemed unethical (e.g., spam, profanity, sexual content, gaming)
- to show unauthorized sites (e.g., pornography, streaming video, E-Bay)
- to show unauthorized services (e.g., peer-to-peer, distributed computing)
- to define proper e-mail use and restrictions (e.g., mass mailing, hoaxes, autoforwarding)
- to explain expected results of policy violations (1st, 2nd, 3rd, etc.)

(Note: Activity in any criteria can lead to criminal offenses.)

q. The authority for soliciting your social security number (SSN) is EO 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose information could result in denial of access to (*insert your organization*) information systems.

7. Acknowledgement. I have read the above requirements regarding use of (*insert your organization*) access systems. I understand my responsibilities regarding these systems and the information contained in them.

insert name here Directorate/Division/Branch	*insert date here* Date
insert name here Last Name, First, MI	*insert Rank/Grade and SSN here* Rank/Grade/ SSN
insert signature here Signature	*insert phone number here* Phone Number

Figure B–1C. Acceptable Use Policy-Continued

Appendix C
Management Control Evaluation Checklist

C–1. Function

The function covered by this checklist is the administration of the Army Information Assurance Program.

C–2. Purpose

The purpose of this checklist is to assist assessable unit manager and management control administrators in evaluating the key management controls outlined below. It is not intended to cover all controls.

C–3. Instruction

Answers must be based on the actual testing of key management controls (for example, document analysis, direct observation, sampling, simulation, or others). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key management controls must be formally evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2–R

(Management Control Evaluation Certification Statement). DA Form 11–2–R is available on the APD Web site (www.apd.army.mil).

a. Have appropriate security personnel (for example, IAPMs, IAMs, or IASOs) been appointed?

b. Have risk analyses and vulnerability assessments been performed for systems that process, access, transmit, or store Army information?

c. Are the appropriate leadership and management personnel aware of the results of risk analyses and vulnerability assessments?

d. Have vulnerability assessments been performed as per standard Army methodologies as detailed in this regulation to ensure consistency?

e. Have countermeasures been identified based on the results of risk analyses and vulnerability assessments?

f. Are countermeasures in place commensurate with risks and vulnerabilities?

g. Is there a written security plan to document implementation of countermeasures?

h. Has leadership and management formally accepted the risk to process the information involved (or more precisely stated: “Are the systems accredited”?)?

i. Are countermeasures routinely tested (for example, user IDs, passwords, audit trails)?

j. Is Information Assurance training being performed?

k. Are MACOMs, installations, or activities identifying their IA requirements under the appropriate MDEP?

l. Are security incidents and violations (for example, viruses, unauthorized access, or attempts) reported?

m. Have plans been developed to ensure continued operation in the event of major disruption (for example, fire, natural disaster, bomb threat, civil disorder)?

n. Has a configuration control board approved each network?

o. Is there an appropriate security official as a member of each board?

p. Is there a current SSAA on file for each IS?

C–4. Comments

Help to make this a better tool for evaluating management controls. Submit comments to: Chief Information Officer/ G–6 (CIO/G–6), 107 Army Pentagon, Washington, DC 20310–0107.

Glossary

Section I
Abbreviations

AAFES
Army and Air Force Exchange Service

ACERT
Army Computer Emergency Response Team

ACL
access control list

ADP (replaced by IT)
automated data processing

AEI
Army Enterprise Infostructure

AES
Advanced Encryption Standard

AIAP
Army Information Assurance Program (replacement for AISSP, Army Information Systems Security Program)

AISSP
Army Information Systems Security Program (replaced by AIAP)

AKO
Army Knowledge Online

AMC
Army Materiel Command

ANOSC
Army Network Operations and Security Center

AOR
area of responsibility

AR
Army Regulation

ARL
Army Research Laboratory

ASA(ALT)
Assistant Secretary of the Army for Acquisition, Logistics, and Technology

ASC
Army Signal Command

ATS
Automated Tactical System

AT/FP
antiterrorism/force protection

ATO
authority to operate

AUP
Acceptable Use Policy

AV
Anti Virus

AWRAC
Army Web Risk Assessment Cell

AWS
Automated Weapons System

BBP
Best Business Practices

BPA
Blanket Purchase Agreement

C4IM
Command, Control, Communications, and Computers for Information Management

CA
Certification Authority (DITSCAP)

C&A
certification and accreditation

CAR
Chief, Army Reserve

CCB
Configuration Control Board

CCI
controlled cryptographic item

CCIU
Computer Crime Investigative Unit

CECOM
U.S. Army Communications-Electronics Command

CI
counterintelligence

CID
Criminal Investigation Command

CIO
chief information officer

CISS
Center for Information Systems Security

CMB
Configuration Management Board

CNA
computer network attack

CND
computer network defense

CNO
computer network operations

CNSS
Committee on National Security Systems

COMSEC
communications security

COOP
Continuity of Operations Plan

COR
contracting officer's representative

COTS
commercial off-the-shelf

COOP
Continuity of Operations Plan

CPP
Cooperative Program Personnel

CRD
compliance reporting database

CSLA
Communications Security Logistics Agency

CT1S
Common Tier 1 System

CT&E
certification, test and evaluation

CVT
Compliance Verification Team

DAA
designated approving authority

DBA
database administrator

DCE
distributed computing environment

DCID
Director, Central Intelligence Directive

DCS
Deputy Chief of Staff

DDL
Delegation of Disclosure Authority Letter

DES
data encryption standard

DIA
Defense Intelligence Agency

DIAM
Defense Intelligence Agency Manual

DiD
Defense in Depth

DISA
Defense Information Systems Agency

DISA/CISS
Defense Information Systems Agency/Center for Information System Security

DISN
Defense Information Systems Network

DITSCAP
DOD Information Technology Security Certification and Accreditation Process

DITYVAP
Do-it-Yourself Vulnerability Assessment Program

DMZ
demilitarized zone

DNS
Domain Name Service

DOD
Department of Defense

DODD
Department of Defense Directive

DODI
Department of Defense Instruction

DODIIS
Department of Defense Intelligence Information System

DOHA
Defense Office of Hearings and Appeals

DOIM
Director of Information Management

DRU
direct reporting unit

EIO&M
engineering, implementation, operation, and maintenance

EKMS
Electronic Key Management System

EOIS
Employee Owned Information System

ESEP
Engineer and Scientist Exchange Program

FLO
foreign liaison officer

FN
foreign national

FOIA
Freedom of Information Act

FOT&E
follow-one test and evaluation

FOUO
For Official Use Only

FPAT
Force Protection Assessment Team

FTP
File Transfer Protocol

GiG
Global Information Grid

GOTS
Government off-the-shelf

HQDA
Headquarters, Department of the Army

I&A
identification and authentication

IA
Information Assurance

IAD
Information Assurance Directorate

IAM
Information Assurance manager

IANM
Information Assurance network manager

IANO
Information Assurance network officer

IAPM
Information Assurance Program manager

IASO
Information Assurance security officer

IATC
interim authority to connect

IATO
interim approval to operate

IATT
Information Assurance Technical Tip

IAVA
Information Assurance Vulnerability Alert

IAVB
Information Assurance Vulnerability Bulletin

IAVM
Information Assurance Vulnerability Management

IDS
Intrusion Detection System

IMA
Installation Management Agency

INFOCON
Information Operations Condition

INFOSEC
Information Security

INSCOM
United States Army Intelligence and Security Command

IO
information operations

IOT&E
initial operational test and evaluation

IOVAD
Information Operations Vulnerability Assessments Division

IP
Internet Protocol

IS
information system

ISP
Internet service provider

ISS
Information Systems Security (replaced by Information Assurance)

IT
Information Technology (replaces ADP)

JIM
Joint Interagency and Multinational

JDSCISSS
Joint DODIIS Cryptologic SCI Information Systems Security Standards

JKMIWG
Joint Key Management Infrastructure Working Group

JTA–A
Joint Technical Architecture-Army

JWICS
Joint Worldwide Intelligence Communications System

KMEC
Key Management Executive Committee

KMI
key management infrastructure

KVM/KMM
keyboard, video, mouse/keyboard, monitor, mouse

LAN
local area network

LE
law enforcement

LCERT
Local Computer Emergency Response Team

LOC
level of confidentiality

MAC
mission assurance category

MACOM
major Army command

MCEB
Military Communications Electronics Board

MDEP
management decision package

MDID
market driven/industry developed

MEVA
mission essential vulnerable area

MOA
Memorandum of Agreement

MOU
Memorandum of Understanding

MPE
miscellaneous processing equipment

MPEP
Military Personnel Exchange Program

MSC
major subordinate command

MWR
morale, welfare, and recreation

NA
network administrator

NAC
National Agency Check

NACIC
National Agency Check with Credit Check and written inquiries

NACLC
National Agency Check with Local Agency and Credit Checks

NDI
non-developmental item

NETCOM
Network Enterprise Technology Command

NETOPS
network operations

NGB
National Guard Bureau

NIPRNET
Unclassified but Sensitive Internet Protocol Router Network (formerly the Non-Classified Internet Protocol Router Network)

NIAP
National Information Assurance Partnership

NIST
National Institute of Standards and Technology

NSA
National Security Agency

OCA
original classification authority

OISS
Operational Information Systems Security

OPCON
operational control

OPM
Office of Personnel Management

OPSEC
Operations Security

ORD

operational requirements document

PAO

public affairs officer

PDA

personal digital assistant

PDS

Protected Distribution System

PED

personal electronic device or portable electronic device

PEG

program evaluation group

PEO

program executive officer

PIN

personal identification number

PL

public law or protection level

PM

program manager or project manager or product manager

POM

program objective memorandum

PPS

ports, protocols, and services

RA

remote access

RADIUS

Remote Authentication Dial-in User System

RAS

remote access server

RCERT

Regional Computer Emergency Response Team

RCIO

regional chief information officer

RDT&E

research, development, test, and evaluation

ROM

read only memory

SA

Systems Architecture or Systems Administrator

SABI
secret and below interoperability

SAP
Special Access Program

SBU
Sensitive but Unclassified (obsolete term)

SCE
service cryptologic element

SCI
sensitive compartmented information

SIGINT
signals intelligence

SII
Statement of Intelligence Interest or Security/Suitability Investigations Index

SIO
senior intelligence officer

SIOP–ESI
Single Integrated Operational Plan-Extremely Sensitive Information

SIPRNET
Secret Internet Protocol Router Network

SIR
serious incident report

SFTP
Secure File Transfer Protocol

SISS
Subcommittee for Information Systems Security

SOP
standard operating procedure

SSAA
System Security Authorization Agreement

SSBI
single-scope background investigation

SSH
secure shell

SSL
secure sockets layer

SSN
social security number

SSP
System Security Policy

STANREP
standardization representative

STEP
standard tactical entry point

STIG
Security Technical Implementation Guide

STS
Subcommittee for Telecommunications Security

TA
technical advisory

TAG
technical advisory group

TEMP
Test and Evaluation Master Plan

TLA
Top Layer Architecture

TNOSC
Theater Network Operations and Security Center

TRADOC
United States Army Training and Doctrine Command

TRANSEC
transmission security

TS
Top Secret

TSACS
Terminal Server Access Control System

TSMB
Tier 1 System Management Board

TS/SCI
Top Secret/Sensitive Compartmented Information

TTP
tactics, techniques, and procedures

UCMJ
Uniform Code of Military Justice

URL
universal resource locator

USAAA
United States Army Audit Agency

USACE
United States Army Corps of Engineers

USAR
United States Army Reserve

USERID
user identification

VAT
vulnerability assessment technician

VIS
vendor integrity statement

VPN
virtual private network

WAN
wide area network

WLAN
wireless local area network

WWW
World Wide Web

Section II
Terms

Access
(IS) Ability and means to communicate with (that is, provide input to or receive output from), or otherwise make use of any information, resource, or component in an IS. (COMSEC) Capability and opportunity to gain knowledge or to alter information or materiel.

Access control
The process of limiting access to the resources of an IS only to authorized users, programs, processes, or other systems.

Accountability
(IS) Property that enables auditing of activities on an IS to be traced to persons who may then be held responsible for their actions. (COMSEC) Principle that an individual is responsible for safeguarding and controlling of COMSEC equipment, keying materiel, and information entrusted to his or her care and is answerable to proper authority for the loss or misuse of that equipment or information.

Accreditation
A formal declaration by a designated approving authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards.

Accreditation authority
Synonymous with designated approving authority (DAA).

Approval to operate
Synonymous with accreditation.

Army information
Information originated by or concerning the U.S. Army.

Audit
Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit trail
Chronological record of system activities to enable the construction and examination of the sequence of events or

changes in an event (or both). An audit trail may apply to information in an IS, to message routing in a communications system, or to the transfer of COMSEC materiel.

Authenticate
To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to possible unauthorized modification in an automated information system, or to establish the validity of a transmitted message.

Authentication
Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's identity or eligibility to receive specific categories of information or perform specific actions.

Auto-manual system
Programmable, hand-held COMSEC equipment used to perform encoding and decoding functions.

Automated information system (obsolete term)
(See information system (IS))

Automated tactical system (ATS)
Any IS that is used for communications, operations, or as a weapon during mobilization, deployment, or a tactical exercise. An ATS may include, but is not limited to, data processors, firmware, hardware, peripherals, software or other interconnected components and devices (for example, radar equipment, global positioning devices, sensors, guidance systems for airborne platforms).

Automated weapon systems (AWS)
Any weapons system that utilizes a combination of computer hardware and software to perform the functions of an information system (such as collecting, processing, transmitting, and displaying information) in its operation.

Availability
The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.

Category
Restrictive label that has been applied to both classified and unclassified data, thereby increasing the requirement for protection of, and restricting the access to, the data. Examples include sensitive compartmented information, proprietary information, and North Atlantic Treaty Organization information. Individuals are granted access to special category information only after being granted formal access authorization.

Central computer facility
One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area. Central computer facilities are those areas where computer(s) (other than personal computer(s)) are housed to provide necessary environmental, physical, or other controls.

Certification
Comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Certification authority (CA)
Individual responsible for making a technical judgment of the system's compliance with stated requirements by identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.

Classified defense information
Official information regarding the national security that has been designated top secret, secret, or confidential in accordance with Executive Order 12356.

Clearing
Removal of data from an IS, its storage devices, and other peripheral devices with storage capacity in such a way that the data may not be reconstructed using normal system capabilities (for example, through the keyboard). An IS need not be disconnected from any external network before clearing takes place. Clearing enables a product to be reused

within, but not outside of, a secure facility. It does not produce a declassified product by itself, but may be the first step in the declassification process. (See Purge.)

Commercial COMSEC Endorsement Program (CCEP)
Relationship between the National Security Agency and industry, in which the National Security Agency provides the COMSEC expertise (that is, standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product. Products developed under the Commercial COMSEC Endorsement Program may include modules, subsystems, equipment, systems, and ancillary devices.

Communications deception
Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications.

Communications security (COMSEC)
Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. COMSEC includes cryptographic security.

Compartmented mode
IS security mode of operation wherein each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts has all of the following: (1) Valid security clearance for the most restricted information processed in the system; (2) Formal access approval and signed non-disclosure agreements for that information to which a user is to have access; and (3) Valid need-to-know for information to which a user is to have access.

Compromising emanations
Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment. (See TEMPEST.)

Computer
A machine capable of accepting data, performing calculations on, or otherwise manipulating that data, storing it, and producing new data.

Computer facility
Physical resources that include structures or parts of structures that support or house computer resources. The physical area where the equipment is located.

Computer security
Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

Confidentiality
Assurance that information is not disclosed to unauthorized entities or processes.

Configuration control
Process of controlling modifications to a telecommunications or information systems hardware, firmware, software, and documentation to ensure the system is protected against improper modifications prior to, during, and after system implementation.

Configuration management
The management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation of an IS throughout the development and operational life of the system.

Contingency plan
A plan maintained for emergency response, backup operations, and post-disaster recovery for an IS, as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Also known as the Continuity of Operations Plan (COOP).

Controlled access protection
Log-in procedures, audit of security-relevant events, and resource isolation as prescribed for class C2 in DOD 5200. 28–STD (DOD Trusted Computer System Evaluation Criteria), often referred to as the "Orange Book".

Controlled cryptographic item (CCI)
Secure telecommunications or information handling equipment, or associated cryptographic component, that is unclassified but governed by a special set of control requirements. Such items are marked CONTROLLED CRYPTOGRAPHIC ITEM or, where space is limited, CCI.

Countermeasure
An action, device, procedure, technique, or other measure that reduces the vulnerability of an IS.

Cryptographic equipment
Equipment that embodies a cryptographic logic.

Cryptographic
Pertaining to, or concerned with, cryptography.

Cryptography
Principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Cryptology
The science and activities that deal with hidden, disguised, or encrypted communications.

Cryptosystem
Associated COMSEC items interacting to provide a single means of encryption or decryption.

Data security
Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Declassification (of magnetic storage media)
An administrative procedure resulting in a determination that classified information formerly stored on a magnetic medium has been removed or overwritten sufficiently to permit reuse in an unclassified environment.

Dedicated mode
IS security mode of operation wherein each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts has all of the following: (a) Valid security clearance for all information within the system; (b) Formal access approval and signed non-disclosure agreements for the information stored and/or processed (including all compartments, sub-compartments, and/or special access programs): and (c) Valid need-to-know for all information contained within the IS. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

Defense in Depth (DiD)
DiD encompasses a physical and logical structure that requires a layering of security policies, procedures, and technology mechanisms to protect network resources, from the desktop to the enterprise, within and across the enterprise architecture. Layered defenses include, but are not limited to, the installation of IA policy protections complementing the use of proxy services, firewalls, IDSs, implementation of Demilitarized Zones (DMZs), redundant filtering policies across devices, and access control and accountability.

Degauss
Destroy information contained in magnetic media by subjecting that media to high-intensity alternating magnetic fields, following which the magnetic fields slowly decrease.

Demilitarized zone (DMZ)
A small network or computer host that serves as a “neutral zone” between an internal network and the public network. A DMZ prevents users from obtaining direct access to an internal server that may have business data on it. A DMZ is another approach to the use of a firewall and can act as a proxy server if desired.

Denial of service
Result of any action or series of actions that prevents any part of a telecommunications or IS from functioning.

Designated approving authority (DAA)
Official with the authority to formally assume responsibility for operating an IS or network at an acceptable level of risk.

Digital signature
An electronic rather than a written signature used by someone to authenticate the identity of a sender of a message or signer of a document. A digital signature ensures that the content of a message or document is unaltered. Digital signatures can be time-stamped, cannot be imitated by another person, cannot be easily repudiated, and are transportable.

Discretionary access control (DAC)
Means of restricting access to objects based on the identity and need-to-know of users or groups to which the object belongs. Controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (directly or indirectly) to any other subject.

Eavesdropping
Method used by an unauthorized individual to obtain sensitive information (for example, passwords, data) from a network. Eavesdropping techniques include wiretapping, eavesdropping by radio, eavesdropping via auxiliary ports on a terminal, and use of software that monitors packets sent over a network. Vulnerable network programs are telnet and ftp.

Embedded cryptography
Cryptography that is engineered into a piece of equipment or system the basic function of which is not cryptographic. Components comprising the cryptographic module are inside the equipment or system and share host-device power and housing. The cryptographic function may be dispersed if identifiable as a separate module within the host.

Embedded (computer) system
Computer system that is an integral part of a larger system or subsystem that performs or controls a function, either in whole or in part.

Emission security
Protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptographic equipment, ISs, and telecommunications systems.

Enclave
A total network made up of all the interconnected computer systems, communication systems, and network components within some logical boundary, usually a boundary device such as a router or firewall. (Replaced the term system-of-systems.)

Extranet
A private network that uses Internet protocols and the public telecommunications system to securely share information among selected external users. An Extranet requires the use of firewalls, authentication, encryption, and virtual private networks (VPNs) that tunnel through the public network.

File server
Computer hardware used to provide storage for user data and software applications, processing capabilities for user workstations, and (normally) connection and control of workstations to a Local Area Network (LAN).

Firewall
A system or group of systems that enforces an access control policy between two networks with the properties of allowing only authorized traffic to pass between the networks from inside and outside the controlled environment and is immune to penetration.

Firmware
Software that is permanently stored in a hardware device that allows reading and executing the software, but not writing or modifying it.

Foreign exchange personnel
Military members or civilian officials of a foreign defense establishment (that is, a DOD equivalent) who are assigned

to a DOD component in accordance with the terms of an exchange agreement and who perform duties, prescribed by a position description, for the DOD component.

Foreign liaison officers (FLOs)
A foreign government military or civilian employee who is authorized by his or her government, and is certified by the DOD Component, to act as an official representative of that government in its dealing with the DOD component in connection with programs, projects, or agreements of interest to the governments. Three types of FLOs include security cooperation, operational, and national representatives.

Foreign national
Non-U.S. citizens who normally reside in the country where employed, though they may not be citizens of that country, and who are employed by the U.S. Government or the Department of the Army to perform services or duties and are not considered a foreign official or representative of that nation.

Foreign official
Non-U.S. citizens who may or may not reside in the country where employed, who are employed by their respective nation as an official representative of that nation in their official capacity, and assigned to the U.S. Government or Department of the Army organizations or commands in the role of liaison, representative, engineer, scientist, or a member of the Military Personnel Exchange Program.

Formal access approval
Documented approval by a data owner to allow access to a particular category of information.

For Official Use Only (FOUO)
DOD information that is not classified CONFIDENTIAL or higher in accordance with DOD 5200.1–R and that may be withheld from public disclosure in accordance with DOD 5400.7–R, which implements the Freedom of Information Act (FOIA). FOUO information, though unclassified, nonetheless is sensitive and warrants protection from disclosure.

Global Information Grid (GiG)
DOD's globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

IA product
Product or technology whose primary purpose is to provide security services (for example, confidentiality, authentication, integrity, access control, or non-repudiation of data); correct known vulnerabilities; or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

IA-enabled product
Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

IAA view
See interconnected accredited IS view.

Interconnected accredited IS view
If a network consists of previously accredited ISs, a Memorandum of Agreement (MOA) is required between the DAA of each DOD component IS and the DAA responsible for the network. The network DAA must ensure that interface restrictions and limitations are observed for connections between DOD Component ISs. In particular, connections between accredited ISs must be consistent with the mode of operation of each IS as well as the specific sensitivity level or range of sensitivity levels for each IS. If a component that requires an external connection to perform a useful function is accredited, it must comply with any additional interface constraints associated with the particular interface device used for the connection as well as any other restrictions required by the MOA.

Information system (IS)
Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and

that includes computer software, firmware, and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems and associated equipment.

Information Assurance (IA)
The protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. This regulation designates IA as the security discipline that encompasses COMSEC, INFOSEC, and control of compromising emanations (TEMPEST).

Information Assurance Vulnerability Management (IAVM)
IAVM is the DOD program to identify and resolve identified vulnerabilities in operating systems. It requires the completion of four distinct phases to ensure compliance. These phases are: (1) vulnerability identification, dissemination, and acknowledgement; (2) application of measures to affected systems to make them compliant; (3) compliance reporting; and (4) compliance verification. This program includes alerts (IAVAs), bulletins (IAVBs), and technical advisories (TAs).

Information dissemination management
Activities to support the management and support of the information and data confidentiality, integrity, and availability, including document management, records management, official mail, and work-flow management.

Information Technology (IT)
The hardware, firmware, and software used as a part of an information system to perform DOD information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

Integrity
The degree of protection for data from intentional or unintentional alteration or misuse.

Intelligence information
Information collected and maintained in support of a U.S. intelligence mission.

Internet
A global collaboration of data networks that are connected to each other, using common protocols (for example, TCP/IP) to provide instant access to an almost indescribable wealth of information from computers around the world.

Intranet
Similar to the Internet, but is accessible only by the organization's employees or others with authorization. Usually internal to a specific organization.

IS security incident
Any unexplained event that could result in the loss, corruption, or the denial of access to data, as well as any event that cannot be easily dismissed or explained as normal operations of the system. Also, an occurrence involving classified or sensitive information being processed by an IS where there may be: a deviation from the requirements of the governing security regulations; a suspected or confirmed compromise or unauthorized disclosure of the information; questionable data or information integrity (for example, unauthorized modification); unauthorized modification of data; or unavailable information for a period of time.

IS serious incident
Any event that poses grave danger to the Army's ability to conduct established information operations.

Key
Information (usually a sequence of random or pseudo-random binary digits) used initially to set up and periodically to change the operations performed in crypto-equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic counter-measures patterns (for example, frequency hopping or spread spectrum), or for producing another key.

Key management
Process by which a key is generated, stored, protected, transferred, loaded, used, and destroyed.

Least privilege
Principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. This also applies to system privileges that might not be needed to perform their assigned job. NOTE: Application of this principle limits the damage that can result from errors, and accidental and unauthorized use of an IS.

Limited privileged access
Privileged access with limited scope (for example, authority to change user access to data or system resources for a single information system or physically isolated network).

Local area network (LAN)
A system that allows microcomputers to share information and resources within a limited (local) area.

Machine cryptosystem
Cryptosystem in which the cryptographic processes are performed by crypto-equipment.

Mainframe
A computer system that is characterized by dedicated operators (beyond the system users); high capacity, distinct storage devices; special environmental considerations; and an identifiable computer room or complex.

Malicious code
Software or firmware capable of performing an unauthorized function on an IS.

Malicious software code
Any software code intentionally created or introduced into a computer system for the distinct purpose of causing harm or loss to the computer system, its data, or other resources. Many users equate malicious code with computer viruses, which can lie dormant for long periods of time until the computer system executes the trigger that invokes the virus to execute. Within the last several years, the Internet has been the conduit of various types of computer viruses. However, there are other types of malicious codes used to cause havoc that are not as well publicized as the virus.

Mandatory access control (MAC)
Means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization (that is, clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity.

Manual cryptosystem
Cryptosystem in which the cryptographic processes are performed manually without the use of crypto-equipment or auto-manual devices.

Military information environment (MIE)
The environment contained within the global information environment, consisting of information systems and organizations-friendly and adversary, military and non-military-that support, enable, or significantly influence a specific military operation.

Multilevel (security) mode
IS security mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts: (a) Some users do not have a valid security clearance for all the information processed in the IS; (b) All users have the proper security clearance and appropriate formal access approval for that information to which they have access; and (c) All users have a valid need-to-know only for information to which they have access.

Multilevel security
Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances, but prevents users from obtaining access to information for which they lack authorization.

Need-to-know
Approved access to, or knowledge or possession of, specific information required to carry out official duties.

Network
Communications medium and all components attached to that medium whose function is the transfer of information.

Components may include ISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

Network management
Activities to support the management and support of the network, including the engineering of changes to the network, maintenance of the network and its components, and user support activities.

Network operations (NetOps)
The organizations and procedures required to monitor, manage, and control the Global Information Grid. Network operations incorporate Network Management, Information Assurance, and Information Dissemination Management.

Network security
Protection of networks and their services from unauthorized modification, destruction, or disclosure. It provides assurance the network performs its critical functions correctly and there are no harmful side effects.

Networthiness
The Networthiness program manages the specific risks associated with the fielding of ISs and supporting efforts, requires formal certification throughout the life cycle of all ISs that use the Infostructure, and sustains the health of the Army Enterprise Infostructure.

Networthiness certification
The Army's networthiness certification process incorporates and demonstrates the completeness of guidance, formats, and practices such as the Army Knowledge Enterprise; the Command, Control, Communications, Computers and Intelligence Support Plan (C4ISP); the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)/System Security Authorization Agreement (SSAA); and existing developmental and operational test requirements.

Non-communications emitter
Any device that radiates electromagnetic energy for purposes other than communicating (for example, radar, navigational aids, and laser range finders). A non-communication emitter may include features normally associated with computers, in which case it must also meet the requirements for an IS.

Non-privileged access
User-level access; normal access given to a typical user. Generally, all access to system resources is controlled in a way that does not permit those controls and rules to be changed or bypassed by a typical user.

Operations Security (OPSEC)
For the DOD components, OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to defense acquisition, defense activities, military operations, and other activities to: (a) Identify those actions that may be observed by adversary intelligence systems; (b) Determine what indicators hostile intelligence systems may obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and (c) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Password
Protected or private character string used to authenticate an identity or to authorize access to data.

PCMCIA
Personal Computer Memory Card International Association is an industry group organized in 1989. The group promoted the standards for a credit-card size memory or input/output device that would fit into a personal computer.

Personal computer (PC)
See information system.

Personal digital assistant (PDA)
A hand-held computer that allows an individual to store, access, and organize information. Most PDAs work on either a Windows-based or a Palm operating system. PDAs can be screen-based or keyboard-based, or both.

Personal electronic devices (PED)
A generic title used to describe myriad available small electronic portable devices that employ the wireless application protocol (WAP) and other “open standards”.

Personal e-mail account
An e-mail account acquired by an individual for personal use. Also know as a private account.

Private account
See personal e-mail account.

Privileged access
Authorized access that provides a capability to alter the properties, behavior, or control of the information system or network. It includes, but is not limited to, any of the following types of access: (a) “Super user,” “root,” or equivalent access, such as access to the control functions of the information system or network, administration of user accounts, and so forth; (b) Access to change control parameters (for example, routing tables, path priorities, addresses) of routers, multiplexers, and other key information system or network equipment or software; (c) Ability and authority to control and change program files, and other users’ access to data; (d) Direct access (also called unmediated access) to functions at the operating-system level that would permit system controls to be bypassed or changed; or (e) Access and authority for installing, configuring, monitoring, or troubleshooting the security monitoring functions of information systems or networks (for example, network or system analyzers; intrusion detection software; firewalls) or in performance of cyber or network defense operations.

Protected Distribution System (PDS)
Wire-line or fiber-optic telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

Proxy server
A server acting on behalf of another server or servers. Such an arrangement allows a single point of entry or exit into a TCP/IP network. A proxy server may also have built-in software that will allow it to be configured to act as a firewall, cache server, or logging server.

Purge
Removal of data from an IS, its storage devices, or other peripheral devices with storage capacity in such a way that the data may not be reconstructed. An IS must be disconnected from any external network before a purge. (See Clearing.)

RADIUS
Remote Authentication Dial-In User Service is a protocol by which users can have access to secure networks through a centrally managed server. RADIUS provides authentication for a variety of services, such as login, dial-back, Serial Line Internet Protocol (SLIP), and Point-to-Point Protocol (PPP).

Remote terminal
A terminal that is not in the immediate vicinity of the IS it accesses. This is usually associated with a mainframe environment and the use of a terminal. Terminals usually cannot operate in a stand-alone mode.

Risk
The probability that a particular threat will exploit a particular vulnerability of an information system or telecommunications system.

Risk assessment
Process of analyzing threats to and vulnerabilities of an information system, and determining potential adverse effects that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective countermeasures.

Risk management
Process of identifying, assessing, and controlling risks arising from operational factors and threats and making decisions that balance risks and costs with mission benefits.

Security guard/filter
IS trusted subsystem that enforces security policy on the data that passes through it.

Security test and evaluation (ST&E)
Examination and analysis of the safeguards required to protect an IS, as they have been applied in an operational environment, to determine the security posture of the system.

Sensitive but unclassified (SBU) (obsolete term)
An obsolete term (in DOD) that has been replaced by sensitive information (see below).

Sensitive information
Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive Information includes information in routine DOD payroll, finance, logistics, and personnel management systems. Examples of sensitive information include, but are not limited to, the following categories: (a) FOUO–in accordance with DOD 5400.7–R, information that may be withheld from mandatory public disclosure under the Freedom of Information Act (FOIA)-see definition above; (b) Unclassified technical data—Data related to military or dual-use technology that is subject to approval, licenses, or authorization under the Arms Export Control Act and withheld from public disclosure in accordance with DOD 5230.25; (c) Department of State Sensitive But Unclassified (SBU)-Information originating from the Department of State (DOS) that has been determined to be SBU under appropriate DOS information security polices; (d) Foreign Government Information-Information originating from a foreign government that is not classified CONFIDENTIAL or higher but must be protected in accordance with DOD 5200.1–R; or (e) Privacy data–-Personal and private information (for example, individual medical information, home address and telephone number, social security number) as defined in the Privacy Act of 1974.

Social engineering
Term used among crackers and security professionals for cracking techniques that rely on weaknesses in process rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system’s security. Classic scams include phoning up a user or helpdesk who has the required information and posing as a field service tech or a fellow employee with an urgent access problem.

SPAM
Unsolicited e-mail received on or from a network, usually the Internet, in the form of bulk mail obtained from e-mail distribution lists or discussion group lists.

Stand alone computer
An automated information system that is physically, electronically, and electrically isolated from all other automated information systems.

Survivability
The ability of a computer communication system-based application to satisfy and to continue to satisfy certain critical requirements (for example, specific requirements for security, reliability, real-time responsiveness, and correctness) in the face of adverse conditions.

Susceptibility
Technical characteristics describing inherent limitations of a system that have potential for exploitation by the enemy.

System
The entire computer system, including input/output devices, the supervisor program or operating system, and other included software.

System architecture (SA)
A description, including graphics, of systems and interconnections, providing for or supporting warfighting functions. It defines the physical connection, location, and identification of key nodes, circuits, networks, and warfighting platforms and specifies system and component performance parameters. It shows how multiple systems within a subject area link and interoperate and may describe the internal construction of operations of particular systems.

System audit
The process of auditing and spot checking to verify secure operation of a system and its support software. If

irregularities are discovered, the audit process includes analysis and identification of the problem, performing corrective actions necessary to resolve the situation, tracking open items actively, and briefing management on identified security deficiencies.

System high (security) mode
IS security mode of operation wherein each user with direct or indirect access to the IS, its peripherals, remote terminals, or remote hosts has all of the following: (a) Valid security clearance for all information within an IS; (b) Formal access approval and signed non-disclosure agreements for all the information stored or processed (including all compartments, subcompartments, and special access programs); and (c) Valid need-to-know for some of the information contained within the IS.

System of systems
A total network made up of all the interconnected computer systems, communication systems, and network components within some logical boundary. (Replaced with the term enclave.)

Terminal Access Controller Access System (TACAS)
A system developed by the Defense Data Network community to control access to its Terminal Access Controllers (TACs).

Technical vulnerability
A hardware, firmware, communication, or software weakness that leaves a computer processing system open for potential exploitation or damage, either externally or internally, resulting in risk for the owner, user, or manager of the system.

Telecommunications
Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

Telecommunications and information systems security
Protection afforded to telecommunications and information systems to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats and to ensure authenticity. NOTE: Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems that generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of technical security materiel and technical security information.

Telecommunications system
Any system that transmits, receives, or otherwise communicates information by electrical, electromagnetic, electromechanical, or electro-optical means. A telecommunications system may include features normally associated with computers, in which case it must also meet the requirements for an IS.

Telnet
A terminal emulation program for TCP/IP networks such as the Internet. Telnet is a common way to remotely control Web servers.

TEMPEST
Short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. (See compromising emanations.)

Terminal
Any device that is used to access an IS, including “dumb” terminals (which only function to access an IS), as well as personal computers or other sophisticated ISs that may access other ISs as one of their functions.

Threat
Capabilities, intentions, and attack methods of adversaries to exploit, damage, or alter information or an information system. Also, any circumstance or event with the potential to cause harm to information or an information system.

Threat agent
A means or method used to exploit a vulnerability in a system, operation, or facility.

Threat analyst
Designated member of the intelligence staff of the supported command of the DAA who will provide the interface on

behalf of DA with the DOD Intelligence Community, the G2, NETCOM/9th ASC, and the intelligence component of the 1st Information Operations Command (Land) to document foreign threats regarding computer network attack (CNA) and computer network exploitation (CNE) or other non-technical threats.

Time bomb and logic bomb
Malicious code that can be triggered by a specific event or recur at a given time. A logic bomb is triggered by an event instead of a specific time. One example of a logic bomb would be a set of programmed instructions to search a company's payroll files, checking for the presence of the programmer's name. Once the programmer ceases employment, the logic bomb is triggered to cause damage to data or software.

Transmission security
The component of COMSEC that consists of all measures designed to protect transmissions from interception and exploitation by means other than cryptographic analysis.

Trapdoor
A hidden software program (potentially embedded into the hardware or firmware) mechanism that causes system protection mechanisms to be bypassed. The code can be hidden in the logon sequence where users are asked to input their user IDs and then passwords. In normal circumstances, the input passwords are checked against stored values corresponding to the user ID; if the passwords are valid, logon proceeds. The trapdoor software would check for a specific user ID, and whenever that user ID is checked, it bypasses the password checking routine and authorizes immediate logon. Trapdoors are sometimes built into development systems by programmers to avoid the lengthy logon procedure.

Trivial File Transfer Protocol (TFTP)
A simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP), a connection-less protocol that, like TCP, runs on top of IP networks. It is used primarily for broadcasting messages over a network and provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers.

Trojan horse
A non-replicating program that appears to be legitimate, but is designed to have destructive effects on data residing in the computer onto which the program was loaded. These programs can perform various malicious activities, such as deleting files, changing system settings, allowing unauthorized remote access, and running malicious programs resulting in destruction or manipulation of data. Trojan horses require user intervention to propagate and install such as opening an e-mail attachment.

User
Person or process accessing an IS by direct connections (for example, via terminals) or indirect connections.

User ID
Unique symbol or character string that is used by an IS to uniquely identify a specific user.

Virtual private network (VPN)
A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Virus
A small program written to alter the way a computer operates without the permission or knowledge of the user. A virus is self replicating with a potentially malicious program segment that attaches or injects itself into an application program or other executable system component and leaves no external signs of its presence, and usually programmed to damage system programs, delete files, create a denial of service, or reformat the hard disk.

Vulnerability
Weakness in an information system, cryptographic system, or components of either (for example, system security procedures, hardware design, internal controls) that could be exploited.

Vulnerability assessment
Systematic examination of an IS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Wide area network (WAN)
A WAN covers a wider geographic area than a LAN, is an integrated voice or data network, often uses common carrier lines for the interconnection of its LANs, and consists of nodes connected over point-to-point channels. Commercial examples are Internet and public data. Government examples are NIPRNET and SIPRNET.

World Wide Web
The universe of accessible information available on many computers spread through the world and attached to that gigantic computer network called the Internet. The Web encompases a body of software, a set of protocols, and a set of defined conventions for accessing the information on the Web. The Web uses hypertext and multimedia techniques to make the Web easy for anyone to roam, browse, and contribute to. The Web makes publishing information (that is, making that information public) as easy as creating a "homepage" and posting it on a server somewhere in the Internet. Also called WEB or W3.

Worm
An independent program that replicates by copying itself from one system to another, usually over a network without the use of a host file. Like a virus, a worm may damage data directly, or it may degrade system performance by consuming system resources or even shutting a network down, but, in contrast to viruses, does not require the spreading of an infected host file. Usually the worm will release a document that already has the "worm" macro inside the document.

Section III
Special Abbreviations and Terms

This section contains no entries.

USAPD

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER WIN32 Version 212

PIN:	081066–000
DATE:	11-17-03
TIME:	16:34:40
PAGES SET:	84

DATA FILE:	C:\wincomp\r25-2.fil
DOCUMENT:	AR 25–2

SECURITY:	UNCLASSIFIED
DOC STATUS:	NEW PUBLICATION